PROTECTING PRIVACY AND PREVENTING MISUSE OF THE SOCIAL SECURITY NUMBER

HEARING

BEFORE THE

SUBCOMMITTEE ON SOCIAL SECURITY

OF THE

COMMITTEE ON WAYS AND MEANS HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

JULY 17, 2000
Delray Beach, Florida

Serial 106–43

Printed for the use of the Committee on Ways and Means

U.S. GOVERNMENT PRINTING OFFICE
66–584 CC WASHINGTON : 2000

COMMITTEE ON WAYS AND MEANS

BILL ARCHER, Texas, *Chairman*

PHILIP M. CRANE, Illinois
BILL THOMAS, California
E. CLAY SHAW, JR., Florida
NANCY L. JOHNSON, Connecticut
AMO HOUGHTON, New York
WALLY HERGER, California
JIM MCCRERY, Louisiana
DAVE CAMP, Michigan
JIM RAMSTAD, Minnesota
JIM NUSSLE, Iowa
SAM JOHNSON, Texas
JENNIFER DUNN, Washington
MAC COLLINS, Georgia
ROB PORTMAN, Ohio
PHILIP S. ENGLISH, Pennsylvania
WES WATKINS, Oklahoma
J.D. HAYWORTH, Arizona
JERRY WELLER, Illinois
KENNY HULSHOF, Missouri
SCOTT MCINNIS, Colorado
RON LEWIS, Kentucky
MARK FOLEY, Florida

CHARLES B. RANGEL, New York
FORTNEY PETE STARK, California
ROBERT T. MATSUI, California
WILLIAM J. COYNE, Pennsylvania
SANDER M. LEVIN, Michigan
BENJAMIN L. CARDIN, Maryland
JIM MCDERMOTT, Washington
GERALD D. KLECZKA, Wisconsin
JOHN LEWIS, Georgia
RICHARD E. NEAL, Massachusetts
MICHAEL R. MCNULTY, New York
WILLIAM J. JEFFERSON, Louisiana
JOHN S. TANNER, Tennessee
XAVIER BECERRA, California
KAREN L. THURMAN, Florida
LLOYD DOGGETT, Texas

A.L. SINGLETON, *Chief of Staff*
JANICE MAYS, *Minority Chief Counsel*

SUBCOMMITTEE ON SOCIAL SECURITY

E. CLAY SHAW, JR., Florida, *Chairman*

SAM JOHNSON, Texas
MAC COLLINS, Georgia
ROB PORTMAN, Ohio
J.D. HAYWORTH, Arizona
JERRY WELLER, Illinois
KENNY HULSHOF, Missouri
JIM MCCRERY, Louisiana

ROBERT T. MATSUI, California
SANDER M. LEVIN, Michigan
JOHN S. TANNER, Tennessee
LLOYD DOGGETT, Texas
BENJAMIN L. CARDIN, Maryland

Pursuant to clause 2(e)(4) of Rule XI of the Rules of the House, public hearing records of the Committee on Ways and Means are also published in electronic form. **The printed hearing record remains the official version.** Because electronic submissions are used to prepare both printed and electronic versions of the hearing record, the process of converting between various electronic formats may introduce unintentional errors or omissions. Such occurrences are inherent in the current publication process and should diminish as the process is further refined.

CONTENTS

PROTECTING PRIVACY AND PREVENTING MISUSE OF THE SOCIAL SECURITY NUMBER

MONDAY, JULY 17, 2000

HOUSE OF REPRESENTATIVES,
COMMITTEE ON WAYS AND MEANS,
SUBCOMMITTEE ON SOCIAL SECURITY,
Washington, D.C.

The subcommittee met, pursuant to notice, at 9:00 a.m., at the City Commission Chamber, 100 N.W. 1st Avenue, Delray Beach, Florida, Hon. E. Clay Shaw, Jr., (Chairman of the Subcommittee) presiding.

[The advisory announcing the hearing follows:]

ADVISORY

FROM THE COMMITTEE ON WAYS AND MEANS

SUBCOMMITTEE ON SOCIAL SECURITY

FOR IMMEDIATE RELEASE
July 10, 2000
No. SS–21

CONTACT: (202) 225–9263

Shaw Announces Hearing on Protecting Privacy and Preventing Misuse of the Social Security Number

Congressman E. Clay Shaw, Jr., (R–FL), Chairman, Subcommittee on Social Security of the Committee on Ways and Means, today announced that the Subcommittee will hold a field hearing on protecting privacy and preventing misuse of the Social Security number (SSN). The hearing will take place on Monday, July 17, 2000, in the City of Delray Beach, City Commission Chamber, 100 N.W. 1st Avenue, Delray Beach, Florida, beginning at 9:00 a.m.

In view of the limited time available to hear witnesses, oral testimony at this hearing will be from invited witnesses only. However, any individual or organization not scheduled for an oral appearance may submit a written statement for consideration by the Committee and for inclusion in the printed record of the hearing.

BACKGROUND:

The SSN was created in 1936 solely for the purpose of tracking workers' Social Security earnings records. However, use of the SSN has expanded significantly beyond its original purpose, and today, it is commonly used as a personal identifier. For example, the SSN is required, by law, for the administration of several Federal programs, such as the income tax, the Food Stamp program, and Medicaid. SSNs are also commonly used in the private sector. For instance, many businesses require that individuals disclose their SSN as a condition for doing business. According to the Social Security Administration (SSA), the SSN is the single-most widely used record identifier in the public and private sectors.

Some believe that the expanded use of the SSN benefits the public by improving access to financial and credit services in a timely manner, reducing administrative costs, and improving record-keeping so consumers can be contacted and identified accurately. Others argue that the pervasive use of SSNs makes them a primary target for fraud and misuse. According to SSA, allegations of fraudulent SSN use such as so-called, "identity theft," increased from 26,531 cases in fiscal year 1998 to 62,000 in fiscal year 1999. Since fiscal year 1999, approximately 1,000 more allegations have been reported each month. In addition to concerns about SSN misuse, privacy concerns have also been raised as companies increasingly share and sell personal information without the customer's knowledge or consent. As a result of these concerns, several proposals have been introduced that would restrict SSN use and protect privacy.

In announcing the hearing, Chairman Shaw stated: "People should have the right to protect sensitive private information, such as their Social Security number. The SSN was never intended to be a personal identifier, yet it has clearly taken on that role over the years. Although the widespread use of SSNs helps individuals in many ways, it also raises serious concerns about privacy and misuse, such as identity theft. We must take steps to protect privacy and prevent fraud while maintaining the legitimate uses of the SSN which benefit the public."

FOCUS OF THE HEARING:

The hearing will focus on the widespread use and misuse of SSNs in the public and private sectors. The hearing will also examine legislative proposals aimed at combating SSN misuse and protecting privacy. The ramification of these proposals on businesses, governments, and consumers will also be examined.

DETAILS FOR SUBMISSION OF WRITTEN COMMENTS:

Any person or organization wishing to submit a written statement for the printed record of the hearing should submit six (6) single-spaced copies of their statement, along with an IBM compatible 3.5-inch diskette in WordPerfect or MS Word format, with their name, address, and hearing date noted on a label, by the *close of business*, Monday, July 31, 2000, to A.L. Singleton, Chief of Staff, Committee on Ways and Means, U.S. House of Representatives, 1102 Longworth House Office Building, Washington, D.C. 20515. If those filing written statements wish to have their statements distributed to the press and interested public at the hearing, they may deliver 200 additional copies for this purpose to the district office of Representative E. Clay Shaw, Jr., 1512 East Broward Blvd., Suite 101, Ft. Lauderdale, Florida 33301, by close of business Friday, July 14, 2000.

FORMATTING REQUIREMENTS:

Each statement presented for printing to the Committee by a witness, any written statement or exhibit submitted for the printed record or any written comments in response to a request for written comments must conform to the guidelines listed below. Any statement or exhibit not in compliance with these guidelines will not be printed, but will be maintained in the Committee files for review and use by the Committee.

1. All statements and any accompanying exhibits for printing must be submitted on an IBM compatible 3.5-inch diskette in WordPerfect or MS Word format, typed in single space and may not exceed a total of 10 pages including attachments. Witnesses are advised that the Committee will rely on electronic submissions for printing the official hearing record.

2. Copies of whole documents submitted as exhibit material will not be accepted for printing. Instead, exhibit material should be referenced and quoted or paraphrased. All exhibit material not meeting these specifications will be maintained in the Committee files for review and use by the Committee.

3. A witness appearing at a public hearing, or submitting a statement for the record of a public hearing, or submitting written comments in response to a published request for comments by the Committee, must include on his statement or submission a list of all clients, persons, or organizations on whose behalf the witness appears.

4. A supplemental sheet must accompany each statement listing the name, company, address, telephone and fax numbers where the witness or the designated representative may be reached. This supplemental sheet will not be included in the printed record.

The above restrictions and limitations apply only to material being submitted for printing. Statements and exhibits or supplementary material submitted solely for distribution to the Members, the press, and the public during the course of a public hearing may be submitted in other forms.

Note: All Committee advisories and news releases are available on the World Wide Web at "http://waysandmeans.house.gov".

The Committee seeks to make its facilities accessible to persons with disabilities. If you are in need of special accommodations, please call 202–225–1721 or 202–226–3411 TTD/TTY in advance of the event (four business days notice is requested). Questions with regard to special accommodation needs in general (including availability of Committee materials in alternative formats) may be directed to the Committee as noted above.

Chairman SHAW. The hearing will come to order. Good morning. I'd like to, first of all, thank the city commission and the mayor for

allowing us to use the beautiful hall here. I was just remarking to Mark that if I was just moving to Florida, this is probably the city I'd settle in. This is really a great community.

When the Social Security numbers were first introduced only six decades ago, their purpose was simple, to keep track of the worker's earnings so benefits could be calculated when the worker retired. The government would even warn individuals to only use their Social Security numbers for purposes of nothing else. As a matter of fact, my Social Security card is a rather old one, I might say, but it also has "not for identity purposes" printed plainly on the face of it.

Today you can barely cash a check or, in my case, I found I couldn't rent a video up in North Carolina without giving this information. In many states, your Social Security number is in plain view on your driver's license. We seldom stop to think how often a number as unique as a fingerprint is a prime target for theft and abuse. Yet theft and abuse of Social Security numbers is happening every day all across America.

Social Security numbers have become the gateway for crooked con artists to raid your bank accounts, max out your credit cards and literally steal your identity. Identity theft is the fastest-growing financial crime in the nation, affecting nearly 600,000 Americans annually.

What was once a form of financial security has become a tool for financial ruin. That's wrong, and that's why last week I, along with a number of my Ways and Means colleagues, including Mark Foley, from both sides of the aisle, introduced legislation that will take some strong steps towards protecting Americans from these rip-off artists. This legislation will prohibit the sale of Social Security numbers and bar their widespread government and public display. It also deters businesses from refusing services to someone who says no to providing their Social Security number.

Additionally, our legislation gives the inspector general new powers to fight fraud and better protect the privacy and integrity of the Social Security number. Finally, penalties and fines are stiffened when the law is broken.

District hearings allow us the unique opportunity to get out of Washington and hear from those citizens on the front line. I look forward to hearing the views and experiences of our expert witnesses, many of whom are our neighbors, as they assist us in finding ways to protect ourselves from identity theft and Social Security number abuse.

Again, I would like to say I'm especially pleased to hold this hearing today in this beautiful city of Delray Beach. I want to thank the city for allowing us the use of this impressive city commission chamber. I think the last time I was in this chamber was to recognize Delray Beach as an All-American City, and that was in 1993, as that plaque says hanging behind me.

[The opening statement follows:]

Opening Statement of Chairman E. Clay Shaw, Jr., a Representative in Congress from the State of Florida

When Social Security numbers were first introduced nearly six decades ago, their purpose was simple—to keep track of a worker's earnings so benefits could be cal-

culated when the worker retired. The government would even warn individuals to only use their Social Security number for this purpose and nothing else.

But today, you can barely cash a check (or in my case, rent a video) without giving this information. In many states, your Social Security number is in plain view on your driver's license. We seldom stop to think of how often a number as unique as a fingerprint is a prime target for theft and abuse. Yet theft and abuse of Social Security numbers is happening everyday in America. Social Security numbers have become the gateway for crooked con-artists to raid your bank accounts, max out your credit cards, and literally steal your identity.

Identity theft is the fastest growing financial crime in the nation—affecting nearly 600,000 Americans annually. What was once a form of financial security has become a tool for financial ruin. That's wrong and that's why last week I, along with a number of my Ways and Means colleagues from both sides of the aisle, introduced legislation that will take some strong steps toward protecting Americans from these rip-off artists.

This legislation will prohibit the sale of Social Security numbers and bar their widespread government public display. It also deters businesses from refusing services if someone says no to providing their Social Security number. Additionally, our legislation gives the Inspector General new powers to fight fraud and better protect the privacy and integrity of Social Security numbers. Finally, penalties and fines are stiffened when the law is broken.

District Hearings allow us the unique opportunity to get out of Washington and hear from those citizens on the front line. I look forward to hearing the views and experiences of our expert witnesses, many of whom are our neighbors, as they assist us in finding ways to protect ourselves from identify theft and Social Security number abuse.

I'm especially pleased to hold this hearing today in the beautiful City of Delray Beach and want to thank the City for allowing our use of this impressive City Commission Chamber.

I'm pleased to introduce my colleague, Mark Foley, a member of the Ways and Means Committee, to this hearing. Mark.

Mr. FOLEY. Thank you, Mr. Chairman. I don't have an opening statement, but I do want to thank you and members of the committee for looking into what is a serious and growing problem in our country relative to the theft of people's personal IDs. As I mentioned during our conference, I myself have been the victim of theft identity, if you will, having had a credit card taken out in my name, using my Social Security number and the fact that I was a government employee in order to gain over $700 worth of merchandise at a store that I do shop at, but never had a credit card issued to me by.

I think clearly the struggles that I undertook in order to clear both my credit and discharge the obligation that was not my own was time-consuming, was frustrating. And it was clearly insulting having a collection agency calling you constantly at home, leaving messages, when you get a live person on the phone, threatening you if you didn't pay your bill that you'd be listed as a deadbeat. It was mind-numbing.

I obviously had the resources and the time to call and continue to pursue and finally get Target, who was most cooperative once I reached their corporate office, discharging the debt. The collection agency, even after I reached Target, consistently tried to call and disrupt me at all hours of the day.

I can only imagine the senior citizen who has had their card stolen having fear of these type of tactics on the phone, threatening that they would lose their home, that they'd lose their credit, that

they'd be taken seriously. And some may even pay the bill that they did not owe simply to get rid of harassers.

I think we've got a multitude of problems here. But most importantly, the age of the Internet, more transactions occurring on computer, I think it's more important than ever that your bill, with the help of Mr. Matsui and others on the Democratic side, be ushered through Congress expeditiously. I think as we take testimony and hear from others, we will probably find out how great a problem this is becoming. A lot of people don't come forward and talk about this simply because they're embarrassed, because the initial thought is oh, I have to report the fact that I didn't pay a credit card, even though it wasn't mine, and that that may jeopardize their credit standing.

Again, Mr. Chairman, thank you for coming and helping on this issue and for the testimony we're looking forward to hearing.

Chairman SHAW. Mark, this matter is becoming even more increasingly difficult and such a growing area of crime. I think that the abuse of the Social Security numbers by just flat-out crooks increased over 200 percent just in this past year. Those are the ones that we know about. Of course, there's many of them going on that we don't know about.

One of our witnesses in Washington had several automobiles purchased in his name and he had his credit card companies after him—or not the credit card companies, but credit bureaus after him. He's still having problems with that thing continuing to pop up. In his instance, it was used as his serial number in the Armed Forces, a colonel in the Armed Forces. On the base at the PX, they required him to show his serial number on the back of a check, which is, of course, his Social Security number. He figures that's probably where his number got out.

This morning our panel of witnesses are composed of Robert Horowitz of Boca Raton, Florida; Carlos Melendez, president of SIC Inc., of Miami, Florida; Douglas Darling, the Director of Florida State Comptroller, Office of Accounting and Auditing. He's with us from Tallahassee. And Wayne Ivey, Special Agent, Florida Department of Law Enforcement, Fort Pierce, Florida. We thank all of you for being with us. We have your full text of your testimony, which will be made a part of the record. And we would ask you to proceed in the way you're most comfortable.

Mr. HOROWITZ.

STATEMENT OF ROBERT HOROWITZ, BUSINESS OWNER, BOCA RATON, FLORIDA

Mr. HOROWITZ. Thank you, Mr. Shaw and Mr. Foley. I appreciate the opportunity you're giving me to read my testimony. I'm going to read off of a prepared text.

My name is Robert Horowitz, a 36-year-old single father of three. I am a homeowner, as well as a business owner, in Boca Raton, Florida. At the end of April 2000, at work, I received a phone call that would change the way I feel about a great many things.

On the phone was a collection agency attempting to collect on a past due debt for several accounts opened with BellSouth Mobility. This was when I was first made aware that someone somehow ob-

tained my personal information, specifically my Social Security number, and my name as it correlates to that number.

I immediately contacted BellSouth Mobility and began the task of cleaning up what I thought was just a reasonable misunderstanding. However, upon speaking with them, I began to realize that what was happening to me was more than some simple error. I was informed that these accounts, five in all, were opened using my Social Security number and my name only. BellSouth Mobility suggested that my credit bureau reports might bear some fruit as to what may also be happening to me.

So I immediately did obtain my credit reports.

Chairman SHAW. Can you check and see if your microphone is on?

Mr. HOROWITZ. It's on.

Mr. FOLEY. We can hear you.

Mr. HOROWITZ. I can speak up a little bit.

Chairman SHAW. As long as the recorder can hear you.

Mr. HOROWITZ. I'm going to turn this off at this point.

Before I even received my credit reports, I was again being contacted by phone and by mail by other collection agencies. And they were all trying to contact me about past-due accounts with other different companies, numerous different companies.

First, let me note that obtaining my credit reports was no easy task. It turns out that the credit bureaus will send you a copy of your report, but they will send it to the most current address on the credit report. In my case, two of the three credit reporting agencies had fraudulent addresses. Therefore, the current address was an address that I had no access to and could not get my credit reports directly. In addition, these credit reporting agencies make it very difficult to communicate with them in any kind of timely fashion. Most things are automated or you have to contact them by way of mail.

Upon receipt, finally, of my credit reports, I was overwhelmed with the amount of incorrect information, as well as fraudulent activity, approximately $15,000 worth of fraudulent activity. How could it be so easy to put fake information on what I thought was my personal credit history? Equally disturbing were that all three credit reports varied a great deal.

For example, Equifax and TransUnion listed me correctly by name and they listed my name correctly only once. However, Experian lists my name nine different times and six of those nine times, my name was spelled wrong. Also, TransUnion had three addresses, one current and two previous, two of which are wrong. And Experian lists 10 different addresses, seven of which are wrong.

After calming down a little bit, I started contacting the companies which I knew were not supposed to be on my credit reports. I also contacted the Palm Beach County Sheriff's Office.

I have since been able to begin the slow process of straightening out my credit reports. In addition, I have kept in touch with Palm Beach County Sheriff's Office. I have come to the conclusion that the police are overwhelmed by this type of crime, simply too many cases and not enough manpower.

I still have a hard time dealing with how easy it was to steal credit or to steal other things using my S.S. number. The only thing they had was my Social Security number and my name. In my case, an American Express card was obtained by way of mail-in application and my name was the only thing correct in addition to my Social Security number. All other information on the application was wrong. My address was wrong. My date of birth was wrong. My phone number was wrong.

As it turns out, all of the fraudulent credit and purchases obtained in my case were obtained in a similar fashion. On all applications for credit, only my first name and Social Security number were correct. All other information was wrong. What puzzles me is why didn't anyone look? Why don't these companies check to see if the information given on these applications correlates to the Social Security number correctly? On every occasion, so much credit was just handed out based solely on my Social Security number, no cross-reference check of any information whatsoever.

Another thing that puzzles me is how quickly and cooperatively these companies are when it comes to clearing up this bad debt; however, uncooperative and completely disinterested they seem to be when it comes to catching the criminal. In fact, it was told to me by more than one of the companies I've dealt with they're not going to attempt to catch the criminal because the amount of fraudulent activity was not significant enough. It was significant enough to send to collection. It was significant enough to have them coming after me and significant enough to have them reporting to credit bureaus; however, not significant enough to try and catch a criminal.

I guess I'm full of old-fashioned thinking, but to me it seems vital to make all attempts to deter this type of criminal activity. If I were a criminal and I knew that as long as I stole a small amount, no one would ever come looking for me, let alone prosecute me. What would be the logic in expecting me to stop doing these crimes? These days, and in the days to come, credit bureaus and their histories and all information are becoming quite a precious commodity.

Certainly, we can foresee a society in the not-too-distant future where we will become cashless altogether. Believing this, we must do more to protect the system of credit. The abuses of the Social Security number as it relates to credit is a problem that's not in the future, however. It is here now.

I am not aware of the current laws as they relate to this issue. I feel that there needs to be a mandatory cross-reference system put into place so that just because someone knows my Social Security number, shouldn't mean they can get credit as they wish. What is wrong, so foreign, about just simply checking all the information available when handing out somebody's credit, not just checking the Social Security number? In my case, every time a person or persons actually approved the credit, they did so without going any further than just checking my Social Security number, even though they had full access to my credit reports.

In closing, I'm told that even if the criminal is apprehended, he most likely will be plea-bargained down and not even have a trial. Again, what kind of deterrent is that? Shouldn't we all be inter-

ested to know where the S.S. number was obtained? In my case specifically, I am told there is nothing, no laws that can force this criminal to tell where he got the S.S. number from. Therefore, my worries are not over. This can keep happening to me even if he is arrested. All one would need to perpetrate these identity crimes is a Social Security number and a name that has good credit.

As a society, we need to come up with a system that does not rely solely on Social Security numbers to obtain somebody's credit or personal information. Until a new and better way is found, I guess we can all expect to be victims.

Again, I thank you for the time.

Chairman SHAW. Thank you, Mr. HOROWITZ. Mr. MELENDEZ.

[The prepared statement follows:]

Statement of Robert Horowitz, Business Owner, Boca Raton, Florida

My name is Robert Horowitz, a thirty-six year-old single father of three. I am a homeowner, as well as a business owner, in Boca Raton, Florida. At the end of April, 2000, at work, I received a phone call that would change the way I feel about a great many things.

On the phone was a collection agency attempting to collect on a past due debt for several accounts opened with "BellSouth Mobility." This was when I was first made aware that someone, somehow obtained my personal information—specifically my S.S. # and my name as it correlates to that number.

I informed the person on the phone that I had never had any accounts with "Bell South Mobility" and began the task of clearing up what I thought was just a simple misunderstanding. However, upon speaking with them I began to realize that what was happening to me was more than a simple error. I was informed that these accounts (five in all) were opened using my credit via my Social Security number. BellSouth Mobility suggested obtaining my credit bureau reports to see if any other unknown activity was taking place.

So I immediately did just that. Yet, even before I received the first credit report. I was again being contacted by phone and mail by other collection agencies about other past due accounts with other companies. [These companies are: again BellSouth Mobility, Burdines, Travelers Bank (Citifinancial) (City Furniture), American Express, BlazerFinancial (Washington Mutual), and Target Stores (Dayton Hudson)].

First, let me note that obtaining my credit reports was not an easy task. It turns out that the credit bureaus will send a copy of one's report only to the most current address on the credit report. In my case, two of the three credit reporting agencies had the fraudulent addresses, being used by the perpetrator, as *my* current address and would only send the reports to this *fake* address. It took much precious time to find this out because as you may be aware, the credit reporting agencies make it very difficult to communicate with them in a timely manner.

Upon receipt of my credit reports, I was overwhelmed with the amount of *incorrect* information as well as fraudulent activity. How could it be so easy to put all this fake information on what, I thought, was my personal credit history. And equally disturbing, all three reports varied greatly.

For example: Equifax and TransUnion list my name correctly and only once, but Experian lists my name *nine* times and six of the nine are spelled wrong. Also, TransUnion lists three addresses (one current and two previous) two of which are wrong. In addition, there are numerous variations from report to report.

After calming down, I started contacting the companies which I knew were not supposed to be on my reports. I also contacted the Palm Beach County Sheriff office.

I have since been able to begin the slow process of straightening out my credit reports. In addition, I have been as active as the law allows in helping the Palm Beach County Sheriff's Office investigate my case. I have come to the conclusion that the police are overwhelmed by this type of crime.

I have a hard time dealing with how *easy* it is to steal credit to steal other things—all one would need is the name and Social Security number of anyone with good credit. In my case, an American Express card was obtained via a mail-in application. I obtained a copy of the application and on it was my name (wrong middle name and last name spelled wrong) and my Social Security number. All other information, i.e. address, date of birth, phone number were wrong!

As it turns out, all of the fraudulent credit and purchases were obtained in a similar fashion. On all applications for credit only my first name and my Social Security number were correct—all other information was wrong. What puzzles me is why didn't any of these companies check to see if my Social Security number correlated correctly with all of the other information given On every occasion, so much credit was handed out based solely on my Social Security number and not on any kind of cross-references.

Another thing that puzzles me is how quickly and cooperatively these companies are too clear the bad or fraudulent debt, but, how slow or uncooperative or completely disinterested these same companies are when it comes to catching the criminal who is actually "stealing" from them. In fact, I was told by more than one of the companies that I've been dealing with, that they are not even going to attempt to catch the criminal because the amount of the fraudulent account wasn't significant enough. Significant enough to send to collections to get the money from me. Significant enough to report to all three credit bureaus, but not significant enough to try to catch the criminal.

I guess I am just full of old-fashioned thinking but to me it seems vital to make any and all attempts to deter this type of criminal activity. If I were a criminal who knew that as long as I stole only a small amount no one would even come looking for me, let alone prosecute me, then what is the logic behind expecting me to sop doing this?

These days, and in the days to come, credit and credit histories are becoming a precious commodity—more now than ever—certainly we can foresee a cash-less society in the not to distant future—believing this, we must do more than ever to protect the system of credit. The abuses of the Social Security number as it relates to credit is a problem that is not in the future—it is here now. I am not aware of the current law as they relate to this issue, however, I feel that there needs to be mandatory cross-reference system put into place so that just because someone knows my Social Security number they shouldn't be able to get my credit to use as they wish. What is so wrong, so foreign, about just simply checking all information available when handing out someone's credit and not just the Social Security number. In every case that, I personally investigated with the fraud using my Social Security number, every single time the person, or persons, who actually approved the credit application did so without going any further than my Social Security number—even though these people had full access to my credit reports.

In closing, I am told that even if the criminal is ultimately apprehended, he most likely will be plea-bargained down and not even have a trial. What kind of deterrent is that?! Shouldn't we all be interested to know where he obtained my Social Security number. In my case specifically, I am told that there is nothing (no laws) to force the criminal to tell where he obtained the Social Security number from, therefore, my worries are not over. If my Social Security number is all one would need to perpetrate these credit crimes or identity crimes, we all need to know the sources of the illegally obtained Social Security number.

As a society we need to come up with a system that does not rely solely on Social Security numbers to obtain someone's credit or personal information. Until a new and better way is found we can all expect to be a victim.

STATEMENT OF CARLOS J. MELENDEZ, PRESIDENT, SIC INC., MIAMI, FLORIDA

Mr. MELENDEZ. Yes, sir. My name is Carlos Melendez. I've been a private investigator in Miami since 1982, started my own agency in '84. The focus of my investigations have been, the majority of them, exactly the kind of problems that the gentleman to my right has been referring to.

As an investigator, I think that the biggest value that I can make to this hearing on behalf of the investigators across this country is to point out that there are approximately 80,000 investigators licensed in the United States presently. They're identifying fraud in the civil sector. The government, quite frankly, is very, very busy involved in looking at criminal behavior. The drugs and all of the major crimes, murder, preoccupy the time for law enforce-

ment to investigate. If Mr. Rosen was to go to the FBI and say I want you to investigate this identify theft that happened or the local police, he would generally not get a favorable response to say "Yeah, we'll go ahead and take that case and we'll go ahead and start investigating it for you now."

So the problem is how do you respond to the theft of the Social Security number. I would also point out that the insurance industry is anywhere from—depending upon job classification listed by the Department of Labor, anywhere from 90,000 to a million people engaged in the business of identifying fraud. The GAO issued a report that talks about $40 billion a year in entitlement fraud and how do these fraud cases happen.

As an investigator and in looking at the problem that I've been asked to comment on today, the privacy issue and identity theft, I think for purposes of definition, it needs to be pointed out that identity theft and identity fraud are two different things. You can have somebody take your Social Security number off of the Internet or steal it from your wallet or steal it from someplace where you're safeguarding the number, but the fact is if he takes it away, that's a theft.

So the question is what is the penalty for him taking your Social Security number? Until that issue becomes a serious enforcement or a serious penalty for him, there's no incentive for him not to go ahead and continue stealing the Social Security number, because nothing's going to happen to him.

I'm not naive to say okay, if we go ahead and say we'll put the guy in jail for a hundred years that that will stop the crime. The punishment, according to criminologists who study these kinds of things, say just by cutting somebody's hand off is not going to solve the issue of theft.

The question then becomes access. As a private investigator, I'm very concerned that in my investigations in my practice that if I don't have as many tools available to me to go ahead and identify—the first thing I do in opening a case is identify the individual and make sure I have the right person. The Social Security number is one of the means to do that, because it's been used as a national identifier for many, many years. The Federal Government in an executive order has got a litany of law that is established as to that. And so it is, in fact, a national identifier, whether we say formally it's not.

So the question is, do you restrict that access to people that are using it that are in the industry and in the business of trying to reduce fraud and theft? My strong message hopefully that will be heard in this hearing is that the private investigator community will not stop their investigations and will not stop finding bad guys just because you can't have access to the Social Security number.

In fact, as I told George during some of our discussions over the phone, what will happen is it will drive the cost of investigating up, because all that's going to happen is we're going to have one less element of information to use in identifying the bad guy. We'll go ahead and go through a process that any good investigator uses in investigating a crime. We'll find the guy. But the Social Security number is one of the things that helps identify without any doubt that this is the bad guy and that is the person.

Then, of course, you get into the situation well, this guy's got many, many Social Security numbers and he's been doing fraud. So now you get on to an investigative run that the gentleman to my right is describing.

George also asked me to speak to some provisions of the law. One of the administrative notes that I will ask—I didn't have a chance to talk to anybody about the law—but it makes reference to the display factor, that you can't have the Social Security number displayed anymore. I would ask the impact on the military? Because, as a retired person, I have a Social Security number on my ID card.

With that, I thank the committee for allowing me to testify.

Chairman SHAW. Thank you.

[The prepared statement follows:]

Statement of Carlos J. Melendez, President, Sic Inc., Miami, Florida

Mr. Chairman.

I wish to thank you and members of the committee for the opportunity to present my testimony. My name is Carlos J. Melendez, President, SIC Inc., Miami, Florida.

I come from a military background, having retired in 1981 after 20 years of service in the Army. I settled in Miami and started my own investigative agency in 1984. I began working as a Private Investigator and Security Consultant, serving corporations, insurance companies, law firms, and private individuals and continue to do so to this day.

I understand the focus of this hearing centers on the national debate on the use of the SSN and the abuses to the Individual's right to "privacy" and protection from a rapidly growing crime called "identity theft".

Put another way, "what would be the impact of legislation prohibiting the sale of the SSN, and, restricting its use to the Private Investigator?"

The short answer is this. If the Private Investigator is found to be abusing the use and access to the SSN, then punish him for violations under applicable law. The obvious observation, why punish all for the mistakes of a few?

On the privacy issue, when conducting an investigation requiring the use of a SSN, Private Investigators already abide by the Federal Trade Commission rules and regulations. Database companies that provide access to their databases which hold the SSN, require Investigators to state the permissible purpose of their inquiry to insure that the purpose meets the criteria established by the provisions of the Fair Credit and Reporting Act.

The practical and direct effect to the consumer of denying access of the SSN to the Private Investigator is: 1) the cost of fraud and abuse losses will go up dramatically; 2) the criminal will have more freedom from detection and will be bolder in deciding to commit crime; and, 3) the cost to investigate fraud and abuse, currently estimated in some quarters to cost society $400 billion in losses, will rise immediately.

In street vernacular, the most significant impact that comes to mind would be, the "bad guys" would win big time!

Why is denying access of the SSN to the Private Investigator even being considered?

In preparing for this hearing, I researched the question of how the Social Security Number (SSN) came to be and why its use became so widespread.

I found that the genesis of the SSN was born with the enactment of the Social Security Act, (P.L. 74–271) (*42 U.S.C. 301 et seq.*) in 1935. While the term "SSN" was not specifically mentioned in the Act, there was authorization to create a means of keeping an accurate record of the earnings of workers covered by the Act.

It wasn't until a year later that a Treasury regulation, "Treasury Decision 4704," required the issuance of an account number to each employee covered by the Social Security program.

However, the SSN began being used in earnest as a "national identifier" in 1943 as a result of the promulgation of Executive Order 9397. The Order required all Federal components to use the SSN "exclusively" whenever the component found it advisable to set up a new identification system for individuals. The Social Security Board was directed to cooperate with Federal uses of the number by issuing and verifying numbers for other Federal agencies. And so the SSN as a "national identifier" was born.

This hearing is a necessary and positive step in responding to the needs of the consumer on the issues, and, represents a reasonable effort to find responsible solutions to the various problems which need to be clearly identified and understood.

In your deliberations, I ask you to consider the make up, number, and nature of work the Private Investigators across this country are performing.

Private Investigators are presently a major crime and fraud fighting force in this country. They are actively engaged on a daily basis in investigating fraud and abuse not currently investigated by law enforcement. Without getting into specific detail, anyone familiar with the differences between law enforcement and private sector investigations understands the roles and missions of each.

Certainly, the Federal agencies; FBI, DEA, IRS, ATF, Customs, and others, are engaged in investigating fraud and abuse. To say otherwise is inaccurate and wrong. It is well known that the focus of law enforcement is primarily on criminal investigations thereby requiring the private sector to initiate private investigations.

The Private Investigative community certainly investigates criminal cases. However, private sector investigations necessarily involve investigating "White Collar crimes" and other so-called "civil investigations" involving fraud and abuse, where Federal, state, and local law enforcement leave off or simply choose not to investigate.

It is well known that Federal law enforcement agencies have an unspoken threshold of dollar value for conducting an investigation. This is recognized by all concerned as simply a matter of allocation of available resources. Thus the private sector is growing exponentially as "white collar" and "civil" crime increases.

Close examination of the ranks of Private Investigators across the country shows, the membership is comprised of a large population of retired and former government service investigators (Federal, state, and local), professionals from the insurance industry, and the legal community. This body of combined experience, clearly demonstrates that today's Private Investigator is a member of a disciplined and professional force. This force is expert with the law and the requirements to respect the Individual's right to privacy. This expertise didn't come about by accident but rather from years of experience gained in his or her previous government service or occupation.

There are numerous professional associations that are dedicated to establishing and maintaining standards for acceptance into membership. There are only 5 states that do not have licensing requirements for Private Investigators. They are Alaska, Colorado, Idaho, Mississippi, and South Dakota.

Thus, Private Investigators are regulated or governed by either State laws or association by laws. Both are vigilant in policing their ranks to insure promulgated laws and regulations are abided by. This regulation protects consumers' rights and provides for sound management of a growth industry that is making a significant contribution to the country.

Meanwhile, out in the field, the Private Investigator is actively engaged in investigating fraud and abuse which is costing the country, hence the population, billions of dollars every year.

Consider the following: 1) the Association of Certified Fraud Examiners reports the figure of $400 billion annually lost to fraud and abuse; 2) Medicare fraud (fraudulent claims) is estimated to be an annual loss of $12 billion; 3) Fraud by Health Care Providers is estimated to cost $95 billion annually; 4) Merchants took in more than $13 billion in bad checks in 1996, an 18 percent increase over the year before, according to the credit industry's Nilson Report, June 1997; 5) Russell Mokhiber (1995), in his article "Soft on crime," states that $200 billion a year is lost to white-collar, or corporate, crime while Josh Martin (1998a), in the more recent article "Dissecting the books," estimates the annual cost to be closer to $400 billion.

Private investigations are being conducted everyday on high dollar losses attributed to money laundering, insurance fraud, medicare/medicaid fraud, credit card fraud, cell phone fraud, identity theft, mortgage fraud, and telephone scams directed at the elderly. Employee theft is major part of the $400 billion dollar loss attributed to fraud and abuse.

Certainly, the obvious impact of denying access of the SSN to the Private Investigator would be to slow down his or her ability to investigate the above described crimes. It most certainly would not stop the investigation. However, the other side of the question is clear. It would be far easier for the criminal to go undetected in the commission of crimes involving fraud and abuse if the Investigator can't find him because of privacy laws. The effect would be that the government would be inadvertently protecting criminals from investigation. Certainly this is not the intention of anyone concerned with fraud, crime, and corruption.

It doesn't take a rocket scientist to conclude that the fraud and abuse numbers cited above would dramatically increase in the billions in annual losses.

But this increased cost can easily be avoided. How?

Continue to allow the Private Investigator access to the SSN as it is currently be used. Regulate and punish abuses by Private Investigators within the existing body of regulation. The Industry is growing. The Federal Government must grow with it.

For example, the Federal Trade Commission (FTC) establishes rules and guidelines for its use. One recent FTC interpretation that appears to have been resolved is classifying the Private Investigator industry as a "Consumer Reporting Agency." While it is understood why this interpretation was made, Private Investigators would consider it ludicrous. The good news is, that it appears that the FTC has accepted the response from the Investigative community through hearings such as this, that an Investigator's report must not be classified as a "Consumer Report," specifically, an Individual's credit report, and is preparing language to reflect the differences.

Anyone familiar with writing rules and regulations for nationwide use is *very* familiar with the care that must be taken for each word and the use of punctuation. That impractical interpretations of the law occur, is understandable. All this means is that a procedure for feedback and response must be available to the consumer to insure bad or ill conceived rules are changed as soon as possible to minimize negative fallout.

The FTC action demonstrates how rules can be amended to reflect practical and workable restrictions enacted to protect the consumer's privacy and at the same time, not enable the criminal more freedom to commit crime.

In polling associates of known or potential abuses of the use of the SSN, some examples were discussed which may need to be investigated. For example, the displaying of the SSN in a bank statement or on a check. In the military, post exchanges require checks be imprinted with the SSN of the person desiring check cashing privilege. These abuses can be administratively corrected by stopping the practice. For example, Florida uses the SSN as part of an identifier in its database but does not print it on the driver's license. This is an example of the responsible management of the database.

The issue of the display of the SSN on a document or in public should be weighed on the occurrence of abuse being experienced. Does it contribute to identity theft? Or does the problem stem from someone who has access to the SSN? Does it stem from access into the database of the institution holding this information simply because he has knowledge of the SSN? In most if not the majority of identity theft cases, the issuing authority of new identification documents failed to check the originating documents to insure their authenticity. Cashing a check without verifying signature or other identifying features such as driver's license happens all the time. False credit card sales without following proper identification procedures is another daily if not hourly occurrence. False credit card sales from collusion from employees with the perpetrator is an example of the classic inside job.

My view is, that the institutions responsible for safeguarding the SSN must be put on notice to safeguard the SSN or it will be done for them.

Then the question becomes, should the consumer have an "opt in or opt out" choice for the use of the SSN? It is also my position that investigation of problems and solutions can be developed to resolve privacy issues and preserve consumer's rights. Each situation must be dealt with on a case by case basis. Only then can you establish rules and regulations to fix the problem.

Another aspect of the question is, how many Investigators, law enforcement and private sector, would this change affect?

The Department of Labor (DOL) web site, proved to be helpful in counting the number of Investigators in the US, *http://stats.bls.gov/oco/ocos125.htm*.

In 1998, police and detectives (law enforcement community) held about 764,000 jobs. NOTE: They are already restricted by laws on the use and sharing of the SSN in an investigation. Adjusters, Investigators, and Collectors," classified by the DOL as administrative occupations, held 1.5 million jobs. Private Detectives and Investigators, classed as a service occupation, held 79,167 jobs. Legal assistants held 85,959 jobs. Claims examiners, property and casualty insurance occupation, held 48,746 jobs.

A quick tabulation shows that in 1998, there were an estimated 977,872 to 1.5 million Investigators asking the same question in the course of an investigation, "do we have the right person?"

The clear implication in changing the law requires careful consideration be given to the number of investigators currently using the SSN in the conduct of an investigation. Will it bring the process to a standstill? The potential cost in time and expense certainly requires serious deliberation.

Identity theft is the other aspect of this hearing. Clearly this is a high priority issue that requires a fix at the earliest possible date. The problem is, the fix must

extend to all the segments of our society that depend on the SSN as an identifier. Supervision and adherence to existing controls would eliminate the majority of violations. Careful handling of the number and its' by the consumer would help. Discovery, access, and the use of the SSN by establishments accepting credit cards is likely the most logical place to start to find ways to stop identity theft.

Thieves, the "fences," and the drug (crack cocaine) sub-culture that thrive on stolen credit cards, passports, and other forms of identification; are not high priority targets for investigation by local law enforcement. Does anyone doubt that the FBI or DEA or local police department could not find a thief who stole your purse or billfold, to include the drug dealer and the fences? Is there any doubt in anyone's mind that they could be found? Then why aren't they being found? Because of the allocation of resources? Go ride with a police officer one day in a major crime area to appreciate what they do. No, the thief is not sought after because he stole a credit card or a purse, he is most likely sought because he seriously injured or killed someone in the course of stealing the identity cards.

Until law enforcement is given the resources to investigate these types of crimes that give birth to "Identity Theft," then don't expect restricting access of the SSN to be reducing the occurrence or elimination of "Identity Theft" anytime soon.

My experience on the planet so far has clearly demonstrated one constant. If we in the United States mean to do something about it, then it will get done in a manner we can all be proud of.

I am happy to entertain any questions you may have. Thank you for your time. And thank you for this opportunity to contribute in this small way to my country.

Chairman SHAW. Mr. DARLING.

STATEMENT OF DOUGLAS DARLING, DIRECTOR, ACCOUNTING AND AUDITING, OFFICE OF THE FLORIDA COMPTROLLER, TALLAHASSEE, FLORIDA

Mr. DARLING. Mr. Chairman, Mr. Foley, I appreciate the opportunity to appear before this subcommittee. I'm representing both Governor Bush and my boss, Comptroller Bob Milligan.

I'm here in support of the legislation. I think that from the Federal level, you have a responsibility, as do we at the local and State level, to protect our citizens. As Governor Bush and Comptroller Bob Milligan's initiative to bring government to the people, one of the ways we're going to do that is by using the Internet.

I think the Internet is both wonderful and frightening when you think about all the information that someone can find out about any of us in this room. And I think that by limiting access to the Social Security number as proposed in this legislation, would help prevent some of the identity theft and identity fraud that's being talked about.

I think the other thing that I would like to leave with you is that from the State level, at least, we take the lead from the Federal Government. Whether we want to admit it or not, as Mr. Melendez said, the Social Security number is the key data element for identification in any system, in any procedure, in any application, as required by the Federal Government. I support your legislation because of that very fact.

You can't get a Federal grant, you can't get a student loan, you can't get a driver's license, you can't get a post office box, you can't get anything without providing your Social Security number. That's not a problem. But what's happened to your Social Security number after that is where the problem comes in. I think the next speaker is going to talk about some of those problems.

One other suggestion that I would like to make, and that is the legislation does not prohibit someone from giving a Social Security number away for free. It just says they can't provide it for anything of value. Maybe another thing to look at would be to add a sentence or two about providing the information, period.

Again, I thank you for this time.

[The prepared statement follows.]

Statement of Douglas Darling, Director, Accounting and Auditing, Office of the Florida Comptroller, Tallahassee, Florida

Mr. Chairman and members of the subcommittee, my name is Douglas Darling. I am the Director of Accounting & Auditing in the Florida Comptroller's Office. I am here representing Florida Comptroller Robert Milligan and Governor JEB Bush in support of proposed legislation to enhance privacy protection and reduce the misuse of social security numbers.

We support the proposed legislation because it appears to provide additional safeguards for our citizens without unduly restricting the use of social security numbers for legitimate government use. I would like to address some issues with the subcommittee on how the State of Florida uses social security numbers for the benefit of our citizens.

In many instances, states follow the lead of the Federal Government. This is particularly true in using the social security number for identification, income tax reporting, and entitlement programs. In any automated system, certain information is critical to ensure data integrity. Most Federal systems use the social security number as that key element of information. Consequently, this precedent has required states to design systems that also report and track using social security numbers. This is not inherently bad. Unfortunately, as addressed by this proposed legislation, when social security numbers are used for unlawful purposes catastrophic results can occur. One of the many valid uses of social security numbers in Florida has resulted in providing support for some of our most vulnerable citizens.

Since the Florida Department of Revenue assumed operational control of Child Support Enforcement, we have been extremely successful in tracking "dead-beat" parents. The key element in our success is the use of social security numbers. Without the ability to monitor earnings and verify current addresses, helping custodial parents would be nearly impossible.

Another use of the social security number by states has increased public safety. Drivers' licenses issued by states use the social security number as a cross reference. This helps prevent individuals whose license has been revoked from simply applying in another state.

Another reason we support this proposed legislation is our unique "Sunshine Law." Chapter 119, Florida Statutes, Public Records Law, requires Florida Government to conduct it's business in a complete and open forum. Any meeting or document, with few exceptions, is available for public inspection. While this law is one of the foundations for our great state, it may be inadvertently contributing to some of the issues addressed by this proposed legislation. The State of Florida could use this legislation as a catalyst to help further protect our citizens from abuses of identity theft.

In summary, State and local governments have necessary and valid uses for social security numbers in providing services to their citizenry. Any reduction of the governmental uses should be carefully analyzed for impact before restrictions are levied. However, this proposed legislation appears to allow valid use by State and local governments while limiting the availability to unlawful users. It is for these reasons that we can support this proposal.

Chairman SHAW. Thank you.

Mr. IVEY.

STATEMENT OF ROBERT W. IVEY, SPECIAL AGENT, FLORIDA DEPARTMENT OF LAW ENFORCEMENT, FORT PIERCE, FLORIDA

Mr. IVEY. Mr. Chairman and Mr. Foley, I thank you for having us here. I represent the Florida Department of Law Enforcement and more specifically, the law enforcement community as a whole.

Earlier when you were starting the meeting, you addressed a number of the issues that we face from the law enforcement standpoint concerning identity assumption fraud. And each of you shared some comments on the overwhelming effects that it's having on our communities. It's basically, in my opinion with basically 20 years of law enforcement, this is the fastest-growing crime that we're facing at this time from a non-violent standpoint. The individual type of activities that we're seeing range from anything from someone assuming that identity and then using it to purchase a cellular telephone to using that same Social Security number and identity to purchase homes.

We at the Florida Department of Law Enforcement work long-term, protracted cases. For the past seven years, I've been heavily involved in working fraud cases that deal specifically with identity assumption fraud and more specifically with Social Security numbers being utilized in those frauds.

One of the cases that I pointed out in my authored letter to this committee is the Campbell Organization. This organization, within a two-year time frame, did an accumulative amount of $3 million in fraudulent activity with over 150 different victims. Each one of those victims faces the same horrors that Mr. Horowitz shared with us earlier today, trying to get their credit straightened out.

Even more importantly, we've had victims that we continually run their name in the computer to determine if they're wanted for a worthless check or some type of fraudulent activity where the investigative agency didn't recognize that it was fraudulent activity. They thought that actual person had gone in and perpetrated that crime when, in fact, it was somebody that had just assumed their identity.

Imagine being stopped for a normal traffic citation or even a driver's license check and finding out that not only have you been the victim of fraud, but now you're wanted for that victimization. The other horrors that we deal with, they go and on.

This organization specifically purchased everything from cellular telephones, computers, homes, cars. They used all of that equipment to either sell on the street or they had an outlet where they were distributing it outside the country. Again, they reached $3 million in just a short period of time of two years. We knew for a fact that single organization had been in operation for about 10 years and had never been arrested.

Mr. Horowitz pointed out in his statement that they did a small amount of fraud on his account and that that would probably never get them arrested. That is the type of activity that happens. Local law enforcement is so overwhelmed with these type of crimes that they're not able to put it all together and recognize that there's a racketeering-type activity or an organized fraud activity that's taking place.

When a victim finally realizes that their identity has been assumed and someone is utilizing their Social Security number, it's too late. It's three, four months into the ball game before they can even start making notifications to the credit bureaus or the other involved parties. That's when their nightmares really begin.

The impact of this on the law enforcement community is overwhelming. We're working these cases. Everyday we have a new case coming in. I know the local law enforcement officers are dealing with the same fact.

We try and put them together and try and establish these organized frauds, but there's a number of organizations that are functioning out there. The primary item that they need in order to function in this capacity is that Social Security number.

Everything in our society is tracked by that. If I go to register for college today, I can almost assure you that they're going to ask me for my Social Security number. And that therefore, is going to become my student ID number at that point. Anything you do, if you open a local checking account at a local bank, your Social Security number is required. If you go fill out an instant credit application, your Social Security number is required.

With that emphasis being put on identity assumption fraud, we have to facilitate some way to restrict the access to these numbers and perhaps look at penalty enhancements for individuals that use Social Security numbers to facilitate fraudulent activity. Right now the criminal element perceives economic crimes and fraud dealing with identify theft as a low-impact crime. They're not going to get a significant jail sentence for it because it's handled individually. They hit one place here, they get a slap on the wrist so to speak.

We have to address those issues in order to start dealing with this problem. It's overwhelming. Is restricting the Social Security number in itself going to solve this problem? No, I don't think so. But that is a very significant step in that direction, as well as the penalty enhancements and everything that goes along with it.

One of the other items I'd like to present to the Committee is Miss Vala Kodish, who was a victim in the Campbell Organization. She authored a letter that I've made available here today spelling out the individual heartaches that she went through in dealing with all this type of activity. She's asked that I publish that letter here today for your review and consideration.

Basically, in closing, I would ask that this committee consider the ramifications of this type of fraudulent activity, the overwhelming impact that it's having on our community in every respect, from an increase in needed law enforcement to deal with it, from our victims dealing with their identity and credit being destroyed at this point and the heartache that it takes to straighten all of that out.

Thank you, Mr. Chairman.

[The prepared statement follows:]

Statement of Robert W. Ivey, Special Agent, Florida Department of Law Enforcement, Fort Pierce, Florida

My name is Robert W. Ivey and I am currently employed as a Special Agent with the Florida Department of Law Enforcement (FDLE). I am assigned to the Ft. Pierce Field Office and have been so employed for the past seven years. Prior to obtaining employment with FDLE I served as a Detective with the Clay County Sheriff's Office and the Putnam County Sheriff's Office for approximately thirteen years.

In total I have approximately twenty years of Law Enforcement experience that has been primarily dedicated to criminal investigation assignments. My assignments with FDLE have primarily been in the area of Fraud Investigations and have focused on major fraud organizations that target victims through the usage of Identity Assumption Fraud. My experience in this area of criminal investigations has enabled me to provide instruction to various organizations in fraud investigations and the prevention of fraudulent activity. Currently I serve on the Education Committee for the newly developed Strike-force Against Fraudulent Enterprises (S.A.F.E.) that has been initiated by the State of Florida in an effort to combat fraudulent crimes throughout the State of Florida.

Since becoming involved in fraud investigations it has been my experience that Identity Assumption Fraud is the most damaging fraud that is committed in our society. The first victim of this type of criminal activity is the person whose identity has been compromised. The problems for this person begin immediately following the assumption of their identity. If the individuals name is compromised that's one problem but if the person's social security is compromised that creates an entirely different set of problems. This is due to almost everything in our society being connected to our social security number. If I attempt to apply for an instant credit loan I must have my social security number. If I want to purchase a vehicle I must have my social security number. In order to open a checking account at a local bank I need my social security number. Everything in the credit world is attached to this one form of identification. The credit bureaus utilize this number to track a person's credit status making it totally vulnerable when utilized in fraud. The major concern for the victim is not dollar loss. The concern is that because of the fraudulent activity their credit is forever damaged. Today along with my testimony I am also publishing a letter addressed to Congressman Shaw from Vala B. Kodish. Mrs. Kodish was a victim of fraud that was perpetrated against her by members of the Campbell Fraud Organization. This organization was investigated and eventually arrested by FDLE and the Metro Dade Police Department. Most financial institutions and credit card companies recognized the organization as one of the largest fraud organizations that operated in the State of Florida. The organization, their operational procedures and the case outcome are detailed during my statement in an effort to demonstrate the impact that identity fraud can have on our community. Mrs. Kodish is a perfect example of the heartache that is suffered by the victim of this type of crime. Her letter to Congressman Shaw is inclusive of the many problems that are created by having your identity assumed by one of these types of perpetrators. I request that you accept her letter as part of your proceedings as she was unable to attend this meeting due to being out-of-State on vacation during this time frame.

In order to fully explain the impact that this type of crime can have on our society I will utilize case presentation of the Campbell Fraud Organization. The Campbell Fraud Organization primarily operated out of the Miami and Ft. Lauderdale areas of the State of Florida. Their organization existed for the sole purpose of committing identity fraud as a means of support for their family. The organization was comprised of various family members but was primarily directed by FREDDIE CAMPBELL and JEFFREY CAMPBELL, two brothers that had educated themselves in the fraud industry. The organization had operated unobstructed for well over ten years. FDLE initiated their investigation in December of 1995 when the organization committed various fraud-related crimes in the Jensen Beach area of the State of Florida. The investigation revealed a large organization that consisted of almost twenty members that were all involved in identity fraud. This group operated by assuming someone's identity and then using that identity to perpetrate fraudulent transactions in almost every form of fraud imaginable. This included instant credit loans, checking accounts, purchases of vehicles, purchases of computer equipment, credit cards, cellular telephones, and even the purchases of homes. The operation involved three independent groups that had specific assignments. The first group was responsible for obtaining the true identification of the victim. This was accomplished through various means to include burglary, robbery, auto theft, postal theft, infiltration of legitimate employees of banks and credit card companies, and the obtaining of information from existing documents that are readily available through various means. Once this information was collected it would be sold to the second group in the conspiracy that would then compile the information and sell it and various forms of identification to the third part of the organization. The third group is the group that would utilize the information to commit the various acts of fraud.

The fraudulent activity that was committed by this one organization totaled approximately three million dollars in fraudulent loss to various private citizens, companies, and taxpayers in the State of Florida alone. This accumulative figure only covers a time period of December 1995 through April of 1997. The actual figure for this organization would be astronomical if law enforcement could apply the actual

dollar loss over the past ten years. This organization would target citizens that were perceived to have good financial status due to the perception that their credit would be readily available and have a higher threshold for credit approval.

Once the members of this part of the organization were armed with the identity of the victim the fraudulent activity would begin. The subjects would work in teams and travel throughout the State of Florida and other southern states in an effort to perpetrate as much identity fraud as possible. The subjects would often rent a U-Haul truck and travel from the Miami/Ft. Lauderdale area in a northerly direction. The group would attack every mall or merchant store in the area as they traveled through the state. Their target purchases would be directed by either orders for certain items that had been placed with the organization or purchases of high-dollar items that were easily marketed on the street. The organization was also responsible for exporting large amounts of electronic equipment, computers, and other significant items out of the country through a source that was identified pursuant to the conduct of the investigation. The organization would apply for instant credit in many of the fraudulent transactions that required the victim's social security number. Additionally the organization would purchase vehicles in the victim's name that would also require the assignment of a social security number in order for credit approval. In summary the members of the organization could and did purchase anything they needed as long as the victim's credit was clean and they had the proper identification to include the victim's social security number. Since the victim would eventually determine that fraud was being committed in their identity the organization needed a system of checks and balances that would alert them that the identity was no longer clean. This was accomplished by listing a contact telephone number on the credit applications that would be contacted by the merchant whenever the account was identified as fraud. The number was listed as a reference number but was actually a cellular telephone that was operated by the perpetrator of the fraud. When an inquiry was made the perpetrator knew that the name was no longer available to use in fraudulent applications. The organization member would then purchase another form of identification from the middle group and start the process over again. This case involved well over one hundred and fifty separate victims that were all targeted by this organization. The victims ranged in age from 18 to 89 years of age. The victims were from every ethnic background and from almost every type of social economic level that exists in our society. As the investigation progressed I discovered more fraudulent activity and began to realize the impact that identity fraud has on our community. The investigation eventually lead to the issuance of warrants for the perpetrators of the crimes and a two State fugitive search for several of the defendants. While searching for the defendants a cooperating witness who was assisting law enforcement was identified by members of the organization. The witness was subsequently approached by three members of the organization and shot in an effort to keep their location from being compromised. The witness survived the attack and was later available for court proceedings.

The investigative phase of the case lasted approximately two and a half years before the final arrests were made. The case was then prosecuted by the Statewide Prosecutors Office in Ft. Lauderdale, Florida and encountered another two years of prosecution and court hearings. The defendants were charged with Racketeering, Organized Fraud, Forgery, Grand Theft, and various other fraud-related crimes. The case was finally disposed of when all of the defendants pled guilty and were sentenced to lengthy prison sentences in the Florida Department of Corrections.

It is important to understand that there are numerous organizations that operate in our society that are of this same magnitude. Each organization is responsible for the impact that identity assumption crimes have on our everyday lives. It is also important to recognize that many times these types of crimes are worked as individual incidents rather than as organizations that are committing these types of crimes. The victim's in these types of cases are now faced with the uphill battle of trying to recover their good credit name and standing so that they can benefit from the original clean credit record that they once enjoyed. As outlined in the letter by Mrs. Kodish this battle is almost never over and certainly never forgotten. The impact of these types of crimes is far reaching and damaging. Let's first address the problems that face the person who has been the victim of the identity takeover. Their problems do not end with attempting to straighten out their credit status. Throughout the conduct of the investigation we continually had to make sure that our victim's were not wanted by outside agencies who had received worthless check complaints by store owners who were unaware that the true named individual did not issue the check or credit request that had been perpetrated. Imagine the nightmare that is created by this type of criminal activity. Imagine being the victim of this type of crime and then being arrested for a worthless check that you did not write while stopped during a traffic incident or license check. Or think of walking

into your local grocery store and being unable to write a check for a purchase because your credit is bad. The list of nightmares is endless and unpleasant.

As a law enforcement officer with twenty years experience I strongly feel that identity assumption and takeover is fast approaching the most serious non-violent crime challenge that America faces. Fraud eventually effects each one of us as the dollar loss for fraudulent activity has to be made up by the merchant who then charges more to the consumer to recover the loss. If we are going to have a chance at combating this problem I feel that there are several issues that must be addressed. First and foremost is a necessity to restrict the availability of social security numbers and other biographical identifiers that are currently available in our society. As discussed earlier in this statement the social security number has become the single most important piece of identification that we have. Every credit related inquiry is attached to this number and identifier. Identity theft crimes are dependent on this number and would become far more difficult to perpetrate if this number were unavailable or unneeded in certain daily activities. Any effort that would restrict the availability of a person's social security number would aid in combating this increasing problem of identity theft that is faced by law enforcement. By restricting the availability of these numbers we would severely handicap the criminal element in their endeavors to commit identity fraud and other fraud-related activities. While this effort alone would not stop the criminal element from committing identity assumption crimes, it would certainly limit the availability of these numbers to the perpetrators of this type of fraudulent activity. This restriction must address all areas that make social security numbers available to the general public.

While the restriction of social security number availability is an important option to consider, I note that the reality of our society and our commerce is that social security numbers have been widely used by *legitimate* businesses and interests for decades as a means of identifying customer accounts and information. Indeed, the use of social security numbers as an identifying factor is a part of our everyday lives. This being the case, it is likely that attempts to restrict social security number usage will be frustrated by the common availability of those numbers already placed in computers, records, and files. Those inclined to use social security numbers for criminal purposes will be able to secure those numbers easily from the huge inventory of information already existent in which social security numbers have been utilized in one form or another.

Additionally, restricting the use of social security numbers could have the unintended effect of punishing all the legitimate businesses and persons who have never utilized those numbers to steal another's identity or to violate the law. If all the legitimate entities in America were to be required to switch their I.D. systems to something that no longer utilizes social security numbers as a factor in customer or client identification, the costs could be significant.

Given this reality, I suggest you consider enacting a penalty enhancement law that would significantly enhance the penalty for anyone convicted of a crime that involved the unauthorized use of another's social security number or that was in any way facilitated, promoted, or assisted through the unauthorized use of a social security number. Such an enhancement would focus upon those who misuse social security numbers, but would not penalize legitimate business owners and others who are using, and have used for years, our social security numbers as a means of identifying customer or client record information. Restricting the widespread legitimate usage of social security numbers may be overwhelming and cost prohibitive. The application of penalty enhancement could easily be accomplished by evaluating the types of crimes that so often occur utilizing identity theft and social security number misuse. This type of penalty enhancement would discourage fraudulent activity of this nature and deter criminals who consider this type of activity.

The second effort must be focused on increased penalties and sentences that are the result of crimes that involve identity assumption. Currently economic crimes of this nature are not perceived as a serious threat to society. The sentence for an economic crime is far less than that for a theft or burglary. The majority of the members of the Campbell Fraud Organization had been arrested on multiple occasions for the same types of fraudulent crimes. But because economic crimes generally do not carry a severe penalty the perpetrators received non-prison or jail sentences. One of the subjects in the case had been arrested over thirty times for fraud related felony crimes. That individual never served a day in State prison until this case was charged. This is true of a great deal of perpetrators in the fraud arena. We must address this issue if we are to combat this problem. We must change the penalties for this type of criminal activity so that the criminal element no longer feels that these types of crimes will go unpunished.

In closing I would like to thank Congressman Shaw on behalf of Commissioner Tim Moore and the Florida Department of Law Enforcement for giving the law enforcement community an opportunity to offer input in this matter. Additionally I would ask that this committee strongly consider the massive impact that identity theft crimes has on our society and the potential for crimes of this nature to become the front runner in criminal activity that must be faced by law enforcement.

Chairman SHAW. I have Miss Kodish's letter, which will be made a part of the record without objection. I see she's from Miami Shores, which is part of my congressional district as well as where we're sitting today.

Mr. Ivey, where do you see the main place where the Social Security numbers are obtained? Or is there anything that you can point to as a place where there's more problems than others?

Mr. IVEY. If I continue with the Campbell case, they obtained the information that they needed for their transactions in a number of different areas. Some of those areas were obtained from actual armed robberies of victims where the only thing they were looking for was their Social Security card. They robbed in specific an 89-year-old lady that was held at gunpoint at a gas station while she was filling up her car.

They commit burglaries. They access it through post offices. They access it through local—not local, but through national credit card companies. We've had a number of instances where they've infiltrated those organizations, gotten employees to give them that information. They have people in the post office that intercept packages that appear to be from credit card companies, from government mailings, those type of things. Specifically, they're looking for the Social Security numbers.

We're also seeing a large influx in the gathering of that type of information from the Internet, from other available resources, government documents, college transcripts. The list is endless. It goes on and on. They're basically going to try every avenue possible to get that one significant piece of information, that Social Security number.

Chairman SHAW. Mr. Horowitz, where did you lose yours?

Mr. HOROWITZ. At this point, I don't know.

Chairman SHAW. You don't have any idea? You weren't the victim of a robbery?

Mr. HOROWITZ. No. Nothing was stolen from me. In fact, no mail has ever been missing. I've never misplaced my identification. I watch over it very closely. I'm, at this point, clueless as to how they got it.

I don't purchase anything over the Internet. If I want to get a gallon of gasoline, I need to give somebody my Social Security number. It could have come from my college records. It could have come from my hospital records. It could have come from numerous places. I truly don't know where it came from.

Chairman SHAW. I know my kids would have their grades posted according to their Social Security numbers. They'd have it posted on the——

Mr. HOROWITZ. Readily available. I don't know exactly where mine was taken from

Chairman SHAW. Mr. Melendez, two questions for you with regard to the Social Security numbers that you say that you use in your investigations. One, where do you generally get those numbers when we talked about the Social Security number of the bad guy? And second, when you have the number, what makes you think that you've got the correct number or that this is the correct ID of the person you're after?

Mr. MELENDEZ. For example, if you were to ask me, you have somebody that's committing a mortgage fraud or you have somebody that's been stalking or you have somebody that's committing disability fraud or something like that and you gave me his name, you would give me some of the basic elements of information. In the case of insurance companies, they would give me the Social Security number and they would give me the other information, like date of birth, address, the kind of cars——

Chairman SHAW. The insurance company would have the—I'm not sure what type——

Mr. MELENDEZ. The insurance company would have that. I would have a file from an insurance company investigator and he would have worked up a file based on application information that would have been received in his office through the process of applying for insurance coverage in an application form.

Chairman SHAW. At that point, you've got a name, you've got an address——

Mr. MELENDEZ. Social Security number and date of birth.

Chairman SHAW.—Social Security number and date of birth. How does that help you in developing the case?

Mr. MELENDEZ. Well, it makes sure that I investigate the correct person. I don't want to be investigating somebody else with the same name.

Chairman SHAW. How would you know that?

Mr. MELENDEZ. Well, in Miami there are a lot of folks with the last same name, for example.

Chairman SHAW. I know that. We don't have it tattooed on us. How would you be sure that this was the right guy? How would you use the Social Security number in your investigation?

Mr. MELENDEZ. The Social Security number would be one of the elements of information that I would use. I primarily would rely upon in most cases the driver's license information and the tag.

As an example, when you do a surveillance, one of the first things that you want to make sure that you do is to make sure that you have the right address, that you have the right person. And you verify that through property records, which has nothing to do with the Social Security number. You go and see whether or not the person is, in fact, renting from that address or if he's, in fact, purchased that address. Those are public record type searches that you double-check to make sure that you're not investigating the wrong person.

Chairman SHAW. Are Social Security numbers on any of those documents?

Mr. MELENDEZ. With some. In the Department of Highway Safety and Motor Vehicles in the State of Florida, it is on the driver's license.

Chairman SHAW. Is my Social Security number on my driver's licence?

Mr. MELENDEZ. No. It's in the database, but it does not appear on the driver's license.

Chairman SHAW. Is this database available to anybody who wants to go look at it?

Mr. MELENDEZ. It's public record, yes.

Chairman SHAW. So all of our Social Security numbers are public record in the State of Florida?

Mr. MELENDEZ. Not necessarily, sir. It all depends. For example, if you went to get your driver's license information or your driving record, as an example, you can get it in a three-year or seven-year, to see what your driving record has been, it would be in that publication generally.

Chairman SHAW. If you wanted to get my driver's license information, could you go get it? Mr. MELENDEZ. Oh, yeah. Any person in the country can get it.

Chairman SHAW. I'm missing something.

Mr. Foley. If the gentleman will yield. The problem is in Florida, they were selling driver's licence information. As of six months ago, I think the practice has been stopped. Our very own State agency was transmitting the information you're talking about, including your Social Security number, to outside vendors.

Mr. MELENDEZ. One of the main problems in identity theft in verifying that somebody—in other words, once somebody says they are who they are, how do you authenticate that? Short of an encryption program that authenticates your Social Security number, you have to use other elements of information, where you live, your telephone number, your date of birth, family members, any other information that you would have that I could find in public records.

Then if you give me an authorization to say it's okay for me to interview a university—for example, if you were going through a top-secret clearance, for example, and I was a contract employee—to go investigate if your credentials are correct or if you have friends that would vouch for your reference and your character and those kinds of things, that's where you get other elements of information to verify the person's identity.

Chairman SHAW. Mr. Foley.

Mr. FOLEY. Thank you very much, Mr. Chairman.

I do appreciate the testimony today because it can bring us to many different points of view. Obviously, the Social Security number is vitally important. It consolidates information. Governments need to share it. It can also help in detecting people who are committing fraud or who have bad credit by using a centralized number. So at one point, I see the need for kind of standardized use of the Social Security number as a way to track citizens' activity, not necessarily in a big government way, but to figure out where they're purchasing, how they're repaying, to make certain additional credit is not issued.

It seems to me our biggest problem is, and it happens potentially even at a rental car counter where you are asked your Social Security number. Who knows whether that clerk is not, in fact, writing it down on a separate ledger and taking it with them?

Mr. MELENDEZ.

Mr. MELENDEZ. If I may, just listening from the questions, I think the thing we need to do trying to fix the problem of identity theft and identity fraud, we need to examine the systems—the public records systems, the management systems, the financial systems. For example, I asked George when he first asked me about this question, Who's dying or bleeding? Where is the real pain?

The pain is in—there's 10 areas, according to the IG's office and the Social Security Administration, where there's major abuses. The primary abuse, the principal abuse, is in the financial industry. Now, the financial industry is using the credit cards, the three credit bureaus, because they have a large body of information. So the credit card industry is very definitely trying to fix the problem, because it's in their financial interest to do so.

Now if you talk about the government entitlement programs, where you have identity theft and entitlement fraud occurring, and if it's occurring in large enough numbers, then I think that you look at how do you fix those problems, as opposed to saying let's go ahead and eliminate the Social Security number from being used as an identifier because it's there. If you say you're going to eliminate it, then what you're really in effect saying is you're going to render all of these systems that use it as an identifier as ineffective or useless, unless you replace it with something else.

The final thing that I would say, because of discussion that's being made on the Internet, you need to look at the use of the Social Security number as kind of like an analog historic—a prehistoric way to the way we used to use it. And we need to be looking now, because we depend on vertical and lateral use between systems, whether it be government, whether it be private sector, the insurance industry versus the State versus the Federal Government, we need to have what I would call a digital signature that is the equivalent of an update—the answers to do this are out there. The technology is there to be able to do this. Authentication encryption procedures are out there, as well as the IG's office talking about using fingerprints as a biometric solution.

The solutions are out there. The question is, how do you go ahead and fix it and apply it to all these systems that are using the Social Security number as a national identifier?

Mr. FOLEY. Well, you do mention digital signatures, which is something Congress has undertaken and has passed recently at least in the House. We're moving along on that venue.

The interesting thing, though, you illuminate is another scary aspect, and we probably don't know the total cost to the taxpayers, is how much potential fraud may be in entitlement programs, as you suggest, whether it's through Medicare reimbursements using somebody's Social Security number. There's no way to trigger whether it's fraudulent, because there is no bill necessarily sent to the recipient. Medicare just pays whoever the provider is using the false number.

Mr. MELENDEZ. I'm sure Special Agent Ivey knows of gangs, especially down in the Miami area, because I know about them, that do nothing but go out and send people to go ahead and apply for entitlement programs using phony Social Security numbers. I mean, it's organized.

Mr. FOLEY. Mr. Horowitz also mentioned something that I think is telling that is frightening to me, when you do talk to the credit agencies or to the vendors who are the suppliers of credit, Oh, it's too small to pursue. One of the problems is the person committing the crimes knows that. So they go out and figure out let's run it up to a grand or so knowing they're not going to come after me. It's small change. But it's affecting everyone in the room, because we're paying higher for merchandise, for credit and for prosecution of the rest of it.

One thing that was mentioned—I think Mr. Darling you said it, I think it's important to note and I hope the record will reflect your statement—providing the information free. It's very, very important in this age of trading, bartering, that we don't provide it or allow it as an exchange rather than a fee for service. That's another way they may get around it.

The question I raised the other day in Washington was, What happens if I'm not selling your number, I'm selling your name and the number is attached? Can they get around it in another vehicle? Well, I'm not selling your name or your number in order to obviate the law. I'm selling addresses and a zip code. That can be a potential problem, as well.

Do you see any way to maybe potentially provide some coverage for those areas that you raise?

Mr. DARLING. Mr. Foley, in the State of Florida, we have Chapter 119, which is the Sunshine Law. I absolutely support that concept. Any citizen in this State can ask just about anything of its State government. By law, under penalty of a felony, you provide it. There are very specific exclusions. Cases that are under investigation, certain criminal investigations and things like that are protected until the court issues final order. Then that's public record also. I support that entirely.

But I think one of the responsibilities of government is to take a look at what we are doing and make sure that we are not doing more harm than good. And specifically to your question, I think the legislation could be strengthened just slightly by adding words to the effect that the Social Security number will neither be sold nor provided. And that would fix the situation you just talked about where credit bureaus or whatever are selling this to other customers, where an insurance company is selling its client list that has Social Security numbers on it. Whether they provide it for free or provide it for something of value, if you just prohibit them from passing that along under any circumstances except for their own internal uses, I think it would strengthen it a little bit.

Mr. FOLEY. One of the things I had to do relative to credit was to require them to notify me if somebody made an inquiry now. So it does delay my ability to pursue my own credit application. If you go to a store, they may offer a special, 30 percent off if you get a credit card in this company name. Now, I require credit bureaus to call me to see if, in fact, I made an application. So it extends, if you will, some of the problems associated with obtaining credit.

I wanted to ask Special Agent Ivey, your testimony describes the method used by Campbell organization to defraud the citizens of Florida of 3 million. Can you tell us a little about how these thieves gained access to the identifying information of the victims?

Mr. IVEY. Yes, sir. Basically, there were three working groups within that organization. The first group was responsible solely for obtaining Social Security numbers, driver's license numbers, any type of identity from a victim. They primarily targeted victims that they perceived would have a high credit threshold. That way they could utilize their credit references and everything from that perspective to facilitate the fraud.

The second group would buy that information from the first group. They would then make the fictitious driver's license or counterfeit driver's license, give them outlets to get certain things, passports or whatever. Once they completed the package on that specific identity, they would turn around and sell it to the third group who would actually go out and commit the fraudulent acts.

That group would on many occasions we tracked them through their historical documents and everything they committed, we would basically observe them or have tracked them going from the Fort Lauderdale or Miami area where they resided, renting a U-Haul and traveling up the Eastern Coast of Florida, hitting every mall, every computer store, everything on the way up until they loaded the U-Haul with the items. They either had an already existing order from someone who wanted that specific item or they would package it and ship it out of the country through another outlet.

The first group basically, as I said earlier, they would obtain that information through whatever means possible, whether it was off the Internet, whether it was from stealing mail out of the U.S. Postal Service, from infiltration of credit card companies or insurance companies, armed robberies, burglaries, auto theft. The list just goes on and on.

Mr. FOLEY. I gather from your testimony that the hard-working Americans who have kept their credit records clean are the ones being targeted for theft identity. Once victimized, can a credit record be restored to its original integrity?

Mr. IVEY. Within a long time span, yes, sir.

Miss Kodish describes in her letter to the subcommittee the horrors that she went through. She had always had perfect credit, had worked hard. She shared with me that her mother and father told her that good credit is one of the most important things you can have. She had worked hard to maintain that status.

All of a sudden, this incident occurs and now she was scared to go into the grocery store and attempt to write a check, because they would push it through the TeleCheck or one of the other check verifying systems and it would be kicked out because of her credit status. Her family attempted to purchase a home. Both of them shared a great credit status. And they were declined on the purchase of their home because of the activity.

She went around to the various credit bureaus, gave them business cards with my name on them so they could contact me and determine that she had been the victim of fraud and therefore, it had created her bad credit status. It was just a continuing nightmare.

Even now—she was victimized, I believe, in early 1996. Even now when she attempts to apply for credit, that still appears on

her record. Within a four or five-year time span, it's still maintained on her record.

Mr. FOLEY. Let me ask a final question of you. I know Mr. Shaw has others as well.

You recommended enhanced penalties for identity theft. Our bill currently includes criminal penalties of up to five years imprisonment or up to 250,000 in fines.

Do you think these are sufficient?

Mr. IVEY. I think that's definitely a great step in that direction. As indicated earlier, a lot of the criminal element feels that committing identity theft fraud or any type of fraud for that matter is a low-impact, low-sentence crime. If they go out and they commit an armed robbery, they know, especially here in the State of Florida with the new gun bill, that they're going to face significant incarceration. If they commit a burglary, it's the same thing.

Fraud has always been treated as a less-impacted crime. And generally speaking, they may get arrested for—let's just hypothetically say going into a merchant and attempting to use someone's credit card or attempting to open an instant credit account, that is going to be treated as an isolated incident. And their sentence for that may be community control or maybe probation.

Very rarely does someone have the time to look into these large organizations that are perpetrating frauds against hundreds of victims and not being recognized as an organized crime. If we can increase penalties for each isolated incident or a penalty for utilizing a Social Security number on another type of entity in the perpetration of a fraud, I think it would definitely have an impact in that direction.

Mr. FOLEY. Thank you.

Chairman SHAW. What happened in the prosecution of the Campbell people?

Mr. IVEY. The prosecution was handled by the statewide prosecutor's office out of Fort Lauderdale. We arrested almost 20 defendants in that case. The charges ranged from racketeering, organized fraud, hundreds of grand theft charges that were incorporated into it. As that case continued, we started looking for the subjects to arrest them. They had gotten word that we were investigating them. They fled.

We found someone that was willing to point them out to us or help us trap them, so to speak. They figured out he was cooperating with law enforcement. They approached him and shot him, trying to keep him quiet from pointing them out.

So the charges at that point went up to attempted murder, witness tampering, racketeering. That was only against two of the defendants, the attempted murder and the witness tampering.

In a whole, the organization was facilitated by Jeffrey and Freddie Campbell, two brothers. Each of them received 10 years incarceration in the State of Florida. And they both pled as habitual offenders with 10 years probation pursuant to that. They received pretty significant sentences from that.

Chairman SHAW. When will they be eligible for parole?

Mr. IVEY. Believe it or not, the case started in 1995. We arrested them in 1997. The case was just recently closed, with everyone receiving sentences. Everyone pled guilty. They just started within

the last year to serve their Department of Corrections sentence. We're looking at approximately eight to nine years before they're——

Chairman SHAW. They'll serve eight to nine years?

Mr. IVEY. Yes, sir.

Chairman SHAW. Mr. Darling, let me quiz you just a little bit as to exactly what uses these Social Security numbers are used for in the State. I know with welfare reform and going after the deadbeat dads, we use that as identification to spread across the country so that we can stop them and prohibit them from receiving driver's licenses, even fishing licenses, that we can identify where they are. That's a very important situation as far as being able to find them and have them come up with their obligations for the support of their children.

What are those areas that the State uses that we have to be careful not to interfere with?

Mr. DARLING. Yes, sir. One of the initial concerns we had with the legislation in an earlier version was we didn't feel like it would have allowed us to do the very thing that you just described. Florida, since turning over child support enforcement to the Department of Revenue, has become extremely successful in tracking down child support payments. The way we do that is if you earn wages in the State of Florida, because of the Social Security number being reported to the IRS, the Department of Revenue can find you and can levy fines and can take some of your wages, if you prefer not to do it yourself. We've been very successful in this regard getting support for the children who need it.

I think the legislation as currently written will still allow us to do that. That was one of the things I was wanting to make sure, from the State prospective, you still allowed State and local governments to use that number until some of the other items that Mr. Melendez mentioned are available.

One of the other things I received from Florida's Highway Safety and Motor Vehicles is the ability to use the Social Security number to track down drivers who say, for example, in North Florida would get a drunk driver conviction, then go to Georgia and apply for another license there. Without the Social Security number, there would be no connection between those two states and not keeping those kind of drivers off the road. So it becomes a public safety concern, also.

Chairman SHAW. Mark, do you have anything further?

Mr. FOLEY. I wanted to, if I could, Mr. Chairman, someone who is the audience, Tim Verrill, has given me a Palm Beach Daily News article dated March 9, 1992 that really goes into a little bit more detail on credit history and one court citing when credit bureau information was used adversely in a court of law.

If you have those two documents, if you'd supply them as part of the report to our recording secretary, it would be helpful, at least, because it may lead us in another direction later on.

[The information follows:]

Lawyer: Your credit history easy to trace

By CYNTHIA WASHAM
Daily News Business Editor

Imagine a young woman fresh out of Harvard University's master's in business administration program who is about to land the job of her dreams with a Fortune 500 company. Her grades are tops. Her references are glowing. She shines through three interviews and comes out clean on the drug test. But she's turned away — because of a bounced check and late Visa payment one semester when her scholarship money arrived six weeks late.

"It's happening today," said Lantana lawyer Tim Morell. "Talk about your Orwellian dream."

Moreover, it's legal.

By giving a prospective employer her Social Security number, the woman in this fictitious scenario gave away the key to her entire credit history. The employer is free to reject her simply because he thinks anyone who has bounced a check is likely to steal.

Florida is what Morell calls an "at-will" state, meaning employers can fire people at will. Only firings based on race, sex, national origin, religion or age are prohibited.

The example of the prying employer shows how computer technology has enabled strangers to tap into vast data bases of information that once were considered personal. It's so common that Morell has made computer law and invasion of privacy his specialty.

Anyone who has applied for a credit card or a loan has a file in the computer of a credit bureau. The bureau collects information from banks and other credit lenders. Two major credit bureaus are Credit Bureau Services and TRW Credit Data.

Individual files contain information on the number of credit relationships a person has, his maximum allowable credit, estimated debt, missed payments, bad checks, income and type of business he's in. It also includes a list of every agency that has requested the file. Items of public record, such as bankruptcies, judgments against the person and tax liens, also may be listed.

The information is available to employers, insurers, lenders and anyone else with a business need for the information. All that's needed to obtain the information is a Social Security number.

"Any time you give your Social Security number to someone," Morell said, "ask why."

Computer hackers don't even need to obtain a Social Security number. With just a person's name and previous two addresses, Morell said, a hacker can tap into someone's credit history.

He told of one client who owed a business associate money. The man who was owed went to a friend at a car dealership and had him get the man's credit history from a credit bureau.

If Morell's client applied for a car loan next week, the auto dealer would see on the client's credit file that another dealer recently checked him out for a loan. He would probably suspect the client was turned down.

Insurance companies routinely dig up credit histories of people suing them over personal injuries, Morell said.

"Why should they get this information?" he asked rhetorically. "It's victimizing the victim."

He said they could try to prove that someone is suing because he needs the money to pay an overdue mortgage or loan, for example.

Morell advises people to protect themselves by checking out their own credit file to be sure it's accurate. Many aren't. His own file listed a prior address that he never had and credit information that belonged to his sister, who shares the same last name and first and middle initials.

"Try to find out what's on the credit file," he said. "Most people would be surprised by what's in there."

While people can do nothing about information that may be unflattering but true, they can change anything that is inaccurate or incomplete, he said.

In the Circuit Court of the Fifteenth Judicial Circuit, Palm Beach County, Florida

George O. Plaintiff,
Plaintiff,

vs. Case No.: CL

Lawyer-Defendant, Esq., Credit Bureau Inc.,
Insurance Carrier-Defendant Insurance Company, and Lawyer-Defendant, Law firm-defendant, P.A., Defendants. /

PLAINTIFF'S RESPONSE TO DEFENDANT'S MOTION TO DISMISS AND DEFENDANT'S MEMORANDUM OF LAW SUPPORTING HIS MOTION TO DISMISS

Issue: Whether it is unlawful to intentionally obtain from a credit bureau consumer credit information for use as background information against an averse party in litigation?

Brief Answer: YES. The Fair Credit Reporting Act provides for damages when a "user" willfully and knowingly obtains consumer information from a consumer reporting agency under false pretenses. *Comeaux v. Brown & Williamson Tobacco Co.,* 915 F.2d. 1264, 1273 (USCA 9th Cir. 1990);

"Users" of the credit report include the ultimate destination of the report as well as any persons who acquired the report for others. *Yohay v. City of Alexandria Employees Credit Union,* 827 F.2d 967, 973 (USCA 4th Cir. 1987); *Rylewicz v. Beaton Services, Ltd.,* 698 F. Supp. 1391, 1440 (US Dist. Ct. N.D. II. 1988); *Boothe v. TRW Credit Data,* 557 F. Supp. 66, 71 (US Dist. Ct. S.D.N.Y. 1982).

"The standard for determining when a consumer report has been obtained under false pretenses will usually be defined in relation to the permissible purposes of consumer reports which are enumerated in 15 USC sec. 1618(b)..." *Hansen v. Morgan,* 582 F.2d 1214, 1219(USCA 9th Cir. 1978).

Obtaining credit information on a consumer from a credit reporting agency for litigation purposes against that consumer is not a permissible purpose under the Fair Credit Reporting Act and, therefore, Attorney Lawyer-Defendant and his lawfirm may be held liable for damages including punitive damages and attorney's fees. *Mone v. Dranow,* 945 F.2d 306, 308 (USCA 9th Cir. 1991).

Discussion: The gist of the case against Attorney Lawyer-Defendant and the Lawyer-Defendant, Lawfirm-defendant lawfirm is that they obtained a credit report on George Plaintiff sometime during the pendency of other civil litigation-and, that they obtained this information without George Plaintiff' authorization. The question raised here, is whether this conduct is illegal.

As set forth in *Mone v. Dranow,* the Fair Credit Reporting Act (FCRA) provides in relevant part:

A consumer reporting agency may furnish a consumer report under the following circumstances and no other:

(3) To a person which it has reason to believe-

(A) intends to use the information in connection with a credit transaction involving the consumer on whom the information is to be furnished and involving the extension of credit to, or review or collection of an account of, the consumer; or

(B) intends to use the information for employment purposes; or

(C) intends to use the information in connection with the underwriting of insurance involving the consumer; or

(D) intends to use the information in connection with a determination of the consumer's eligibility for a license ...; or

(E) otherwise has a legitimate business need for the information in connection with a business transaction involving the consumer.

15 U.S.C.'s 1681 b (1982). A consumer whose credit report is obtained for reasons other than those listed in the statute may recover actual and punitive damages and attorney's fees and costs from the user of such information. 15 U.S.C.'s 1681n (1982). *Mone v. Dranow, 307–308.*

Mr. Plaintiff's claims against Attorney Robert Lawyer-Defendant and the Lawyer-Defendant Lawfirm-defendant lawfirm are particularly established through paragraphs 8, 23, 24, and 29. That is, within the context of the Credit Bureau credit report being a consumer report, the allegations are that these defendants acted willfully, with no proper purpose, and did affirmatively conceal and misrepresent the nature of what they had done. That being said and previously sworn to by Mr. Plaintiff, the defendant's factually based claims that the report was not a consumer report and that these defendants did not themselves ask that Mr. Plaintiff's credit report be pulled cannot have any weight on a motion to dismiss:

> A motion to dismiss tests whether a cause of action is stated and requires the court to look only at the four corners of the complaint without considering any affirmative defenses raised by the defendant, or evidence likely to be produced by either side. *Martin v. Principal Mutual Life Insurance Co.,* 557 So. 2d 128, 128–129 (Fla. 3d DCA 1990); quoted from: Florida Civil Practice Before Trial, pp 13–12; *The Florida Bar (1993).*

In any event, there can be no doubt that the Credit Bureau report at issue in this matter was a "consumer report" within the FCRA:

> The term "consumer report" means any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness ... which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (1) credit or insurance to be used primarily for personal, family, or household purposes, or (2) employment purposes, or (3) other purposes authorized under section 1681b of this title ....15 U.S.C.'s 1681a(d) (1988). *Comeaux v. Brown & Williamson Tobacco Co.,supra*,1274.——

What other reason does a credit bureau have for collecting such information? In *Hoke v. Retail Credit Corp. 521 F.2d. 1079 (USCA N.C.1975); cert. den. 96 S.Ct. 878.,* a "consumer report" was held to be virtually any information communicated by a consumer reporting agency about a consumer. Also see *Hall v. Harleyville Insurance Co.;* 896 F.Supp.478, 482 (US Dist. Ct. ED P.A. 1995):

> the FCRA covers actual credit reports because those reports were originally collected for the purposes of determining eligibility for insurance, credit or employment purposes, even if they were not used for those purposes in these particular instances. See *St. Paul Guardian Ins. Co.v. Johnson;* 884 F.2d 881, 883 (5th Cir. 1989); *Ippolito v. WNS, 864 F.2d. 440, 453*(7th Cir. 1988); *Zeller v. Samia,* 758, 780 (D.Mass. 1991).

Attorney Lawyer-Defendant and the Lawyer-Defendant Lawfirm-defendant lawfirm have urged this Court to believe that even if they did obtain Mr. Plaintiff's credit report without his authorization, and even if the purposes for which they obtained the report were improper, the FCRA simply does not apply to either of them.

In particular, Attorney Lawyer-Defendant and the Lawyer-Defendant Lawfirm-defendant lawfirm cite this Court to the case of *Di Carlo v. Focas,* 855 F. Supp. 823 (US Dist. Ct. Md. 1994) and the case upon which *DiCarlo* relied, *Frederick v. Marquette Nat'l Bank,* 911 F.2d 1 (USCA 7th Cir. 1990, citing *Ippolito v. WNS, Inc.* 864 F.2d 440, 7th Cir. 1988).

These cases as applied to the present allegations simply have no merit. The DiCarlo case simply regurgitated the holding in Fredrerick, without any further analysis or review of the existing case law and the Court in *Frederick*: A. Was not briefed on the issues which constituted the basis of its holding; B. Did not properly apply the *WNS* case upon which it allegedly relied and C. Never considered FCRA section 1681 (q) which provides:

> Any person who knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretenses shall be fined not more than $5000.00 or imprisoned not more than a year or both.*

Indeed rather than simply FCRA section 1681 m cited by Attorney Lawyer-Defendant and the Lawyer-Defendant Lawfirm-defendant lawfirm, several sections of FCRA have been held to place requirements of users:

Section 1681 d, 1681 q, and 1981 r. *Rice v. Mongomery Ward,* 450 F.Supp. 668, 670 (US Dist. Ct. MD N.C. 1978)

> Non-compliance with s. 1681q thereby forms the basis of civil liability under 1681 n. [This] construction has been adopted by the other circuits addressing this question. See *Yohay v. City of Alexandria Employees Credit Union, Inc.,* 827 F.2d 967, 972 (4th Cir. 1987); *Zanmora v. Valley Federal Sav. & Loan Ass'n,* 811 F.2d 1368, 1370 (10th Cir 1987)...
>
> *Comeaux v. Brown & Williamson Tobacco Co.,supra, 1274.*

It must be taken as a given that Attorney Lawyer-Defendant and the Lawyer-Defendant Lawfirm-defendant lawfirm could not have obtained George Plaintiff's credit report for any legitimate reason (*Mone v. Dranow)*, therefore a factual question exists as between these lawyers, Insurance Carrier-Defendant, and Credit Bureau as to why Mr. Plaintiff's credit information was unlawfully given out. See *Joseph LETSCHER v. SWISS BANK CORPORATION*; No. 94 Civ. 8277 (LBS) US Dist.Ct.,S.D.N.Y. April 16, 1996.(1996 WL 183019 (S.D.N.Y.))—finding that since discovery had not taken place it would have been improper to grant summary judg-

ment where allegations and inferences therefrom could support claim that defendants used false pretenses to obtain the plaintiff's credit report.

* Although the DiCarlo decision did consider this point, procedurally, the case was in a different posture-ie opportunities to create factual issues had been available in DiCarlo as the matter was determined on motion for summary judgment. In this case, discovery has been suspended by order of the court pending a final determination of the legal entitlement to proceed.

Conclusion: Every Federal circuit court which has considered whether users may be liable under FCRA for intentionally and improperly requesting credit reports has found civil liability as a matter of law (note, in *WNS v. Ipolito*, the court pointed out that under 1681 q, merely obtaining "information on a consumer"—not a consumer report per se—is all that is required to establish liability under the circumstances alleged in the present complaint, See FN 8, page 448).

At this stage of the proceedings, the Court should immediately allow discovery to be taken and the case to proceed on claims for punitive damages as allowed by the Federal law.

Mr. FOLEY. Let me ask Mr. Horowitz, you mentioned that credit bureaus will send a copy of ones credit report to the most current address on the credit report. If the person's identity has been stolen, the false address is the only address the credit bureau will send the report to.

How did you go about resolving this so that you would receive all of your credit reports?

Mr. HOROWITZ. It wasn't easy. I had to mail a letter of request explaining my situation in great detail. At which point, they mailed back to me a request for a couple of bills, like my cable bill, my water bill, to prove that I am, in fact, living where I am living before they would mail me anything to that address.

There was one other thing you mentioned about putting a tag or note on your credit bureau report. I've also done that. I understand you can only do that if you claim to be the victim of fraud, which is strange. I mean, put the ointment on after you've been bit. However, the human factor involved in this, I don't put much credence in those little notes.

My information, in my particular case, it was so blatantly wrong and nobody bothered to check the credit report anyway. So why would I believe they're going to check the credit report to see a little note on there that says, Hey, this is a victim of fraud? They didn't check to see if it was my right birth date, if my name was spelled right. What would make me think they're going to check those little things?

The incentive when you go in to apply for credit, the person behind the counter, I believe there's a financial incentive in most places to get you a credit application and get you approved for credit. This way the employee makes a little extra money each week. That incentive in itself leaves a lot of room for error. If I was told every time somebody gets an application, push, push, push, get it approved and you get an extra 20 bucks, I'd be looking to do that as often as possible. I'd ignore that information.

Mr. FOLEY. One thing that I've noticed as well is the recent surge of credit card applications being mailed to my home in both Washington and in Florida. One concern I have, and I didn't realize this, every time a person inquires as to my credit, it acts, if you will, as a negative on my report.

I tried to apply for credit at one point and somebody said No, you're denied. I said "Why am I denied?" They said because you've had too many inquiries. I said, "Inquiries from who?" They said, well—they sent me a report, and there were places I never heard of.

They inquired on to my credit for either the purposes of soliciting me for a gold platinum super express card with two interest, only for the first three days, then it's 19 after that. But the fact is they apparently applied or tried to gain a view of my credit before they sent the application. That counts as a negative against my score card.

Are you all aware of that?

Mr. MELENDEZ. Yes, sir.

Mr. DARLING. Yes, sir.

Mr. IVEY. Yes, sir.

Mr. HOROWITZ. Yes, sir.

Mr. FOLEY. How can we go about correcting some of that? The false inquiries that I have not authorized seem to be as big a problem as those that are fraudulently taking place.

Mr. IVEY. One area that I think needs to be considered is the credit companies that are facilitating these loans. For example, if I go to a store and I fill out an instant credit application in your name, if I'm the perpetrator of fraud, I'm going to put down some legitimate information that I know is warranted to get the loan approved. At the same time, I'm also going to put down some information that will allow me to have a system of checks and balances, if you will.

An example of that would be a telephone number for a contact. It might be an employer. It might be any number of persons that I list. What I would therefore do with that number is when they realized that fraud has been perpetrated against this account, they're going to take that loan application, they're going to look at it and say here's a phone number. Let's determine if this person works here. They're going to call that number that's been listed. That person may answer the phone in any business name. He may just answer the phone hello. The person that's making the inquiry is then going to say I'm looking for Wayne Ivey or I'm looking for Mr. Foley.

That person at that time knows this account is no longer a good account for me to use. It's been compromised. Now, they go and obtain another account.

One thing that might benefit everyone is if the credit report was inclusive of contact information that is provided by the actual person with that identity. If I have a credit report in my name, there's a contact number at the Florida Department of Law Enforcement. There's a contact number at my home. Then that company, for example the finance company, can look at that credit report and say here's the legitimate information. Here's the information that was provided. Let's call the information that's listed in our credit report. Then they're actually talking to the person.

If that had happened in Mr. Horowitz's case, he wouldn't have the problems he's had at this point.

Mr. FOLEY. Mr. Chairman, the reason for some of these diverse questions is obviously I think we have another mission on our

hands, not only for the sale of Social Security numbers, but a fair credit reporting standard and the way the law applies we're going to have to look at. I think there's a two-prong problem here. One is using the incorrect or correct Social Security number by the person perpetrating the crime.

But also the problems encountering the clearing out, solving the inquiries made to, the granting of credit, the dunning of people, the whole process seems to be particularly for citizens who are maybe more vulnerable and less able. A senior citizen; a mother raising children trying to go to work, raise the kids, get them off to school and, by the way, call a credit reporting company or a harasser or credit collection agency five, eight, 10, 15, 20 times never with a 1–800 number. It's all on your nickel to try to get this thing straightened out.

At times I'm sure people throw up their hands, find themselves then unable to get credit when they desperately need it themselves. They apply for a car, like the person you mentioned, five cars are purchased in your name. So I'm not selling you a car. You've got a bad credit rating. Nothing done by my own initiative, but by a thief. Then all of a sudden, low and behold, the legitimate citizen can't gain access to credit. That's a serious problem.

I think we have a multitude of things we're going to deal with. Hopefully your testimony and your submission to the record will help us in looking through the web of problems that we have.

Chairman SHAW. We're now operating in the Banking Committee.

I don't think you'll get things done quite as quickly over there when you try to get into that area. I've ventured into that maze before. I was amazed to find out how many friends the Banking Committee has to do credit reports.

I'd welcome to do it. I'd like to support you in that effort. I think that the reporting of credit today is so important to all of us. This is a significant first step to halt the use and dispersement of these numbers.

I'm particularly interested in the sunshine law in Florida, which we all support, but there's nothing to be gained by the public having access to people's Social Security numbers. That wasn't what the sunshine law was all about. I think we need to be sure and I'm reasonably sure that we closed that loophole with the legislation that we have. I believe Mr. Darling you testified as such.

One final question. Mr. Ivey, is that a Super Bowl ring you have on your finger?

Mr. IVEY. No, sir. It's from wrestling. I won the World Police Olympics twice.

Chairman SHAW. It looks like a Super Bowl ring. You've got to be a tough dude to wear that.

I'd like to thank all of you for being with us today. This is good information, meaningful information that we can take back to Washington. As a result of this hearing, we'll make some adjustments.

Mr. Melendez, I don't know what we can do to help your situation with regard to the identity. I think that the problems that we might cause you in your investigating process will be more than offset by the problems that we will solve for the Mr. Horowitzes of

the world who find that this information is being distributed. Anyway, as an investigator you'll probably find some way around the legislation anyway, in order to get all the information you need to complete your work.

The Social Security number is being used for many legitimate purposes, which we have to continue to use it for, such as child support enforcement, such as driver's license protection, driver's license identity, whether it be someone who owes child support in prohibiting them from getting a license or whether it be someone going over to another State to get a license where their license has been suspended for some unlawful activity. So we have to be very careful that we don't shut those processes down. Also for purposes of reporting income, banks are still going to need this to report the interest you earn as are other type of agencies, including brokerage offices, I would assume.

The dispersement of the information by other than the person whose number it is, is what we've got to close down. The intergovernmental use of the number I think is protected under this legislation. I'll see that it is. But the dispersement of this and relaying these numbers over to the public is something that we do need to stop.

Again, I thank this panel. You've helped us greatly. With that, I believe that's the only thing we had. The hearing is adjourned.

[Whereupon, at 10:08 a.m., the hearing was adjourned.]

[A submission for the record follows:]

MIAMI SHORES, FLORIDA

To: Congressman Clay Shaw, State of Florida

From: Vala B. Kodish, Miami Shores, FL

Dear Congressman Shaw:

First, let me apologize for the informality of this letter being sent to you via email. Agent Wayne Ivey, FDLE, contacted me about your hearing and I happened to be on vacation out of state. I would prefer to be there in person, as this matter is very important to me.

Please allow me to tell you a little about myself and why this letter comes to you at this time. I am a mother of 3 small children; an employee of a major U.S. corporation; and a partner in my husband's successful business.

Four years ago, Leap Day to be exact, I was taking my two sons to their church preschool in our small community. I remember it well. I had the flu, so I hid my purse in the back of my mini van under some pillows and locked the door. I was out of the car no longer than 2 minutes. When I returned, my purse was gone. I reported it to the local police. Of course I made all the necessary calls to my bank and credit companies. Within days agent Wayne Ivey showed up at my house and told me that he had reason to believe that I had fallen victim to a crime ring. Indeed I had. The mail began to pour in.

At first it was the plastic for credit that had been approved for items bought on the spot...$4,000 worth of leather furniture; then computer equipment; pool supplies, etc. Not long after that I began to receive notices for bounced checks. They even opened an account for company checks based on a fictitious business that I supposedly owned. I spent hours on the phone and sending letters of explanations, along with copies of the police report and the case number that Mr. Ivey had given me. That was all I could do. I was helpless. At one point Mr. Ivey came to me to help him with his investigation and showed me pictures of the woman impersonating me; and of the others that were working with her; along with copies of the fraudulent checks. You have no idea how frightening that was to see all the evidence there before me. Worst of all, they were committing the fraud within my small community and the perpetrators were living within close proximity. I cannot tell you the hours I laid in bed at night worrying they would get just a little more greedy or even curious about me since they knew where I lived.

Then I worried they would be in a fatal accident and I would be blamed for it. I called the State Troopers and they told me it could possibly happen, that I needed

to send them a letter of explanation for their records. Then I went to get a new driver's license. Do you know that they would not give me a new license number even after I told them that the previous number was being used fraudulently by criminals. They told me that under no circumstances do they give new numbers. Then I worried about my Social Security retirement fund. I called the office in Washington and was flabbergasted at what they told me. They said, (to paraphrase) "It is highly unlikely that a criminal would try to receive Social Security benefits. And if you change your number it is possible that your life's earnings may not follow the new number. I wouldn't take that chance." What kind of choice is that!!?? THEY WERE TELLING ME THAT I HAD A BETTER CHANCE TRUSTING THE CRIMINAL THAN THEIR ACCOUNTING SYSTEM! Day by day I began to understand why these criminals were making a living at beating the system. A child could beat this system! There is no way out for the victim. And let me tell you, I have continued to be the victim for these past 4 years. Let me count the ways: I cannot write checks. I have a black mark against my name. In some cases it remains even after I have jumped through all the hoops the credit establishment requires. Therefore, I have to carry cash (which is not an option in Miami) or use credit. Using credit as my only option means I have to pay interest on the charges made. We sold our home for $300,000. A year later we bought a home for $285,000. You would think that we would qualify without a second thought. I spent at least 8 months working on clearing my credit before the new purchase. When it came to shopping the mortgage, I had no choice but to use a mortgage broker because I had one creditor who had bought the debt and actually told me he didn't care if it was fraud or not, he wanted his money and he would not clear my name. As you know, the broker had to take his cut in order to make the transaction, therefore the loan cost us more than if we would have shopped it on our own.

Mr. Shaw, I learned as a child the importance of good credit. I have had the same banking account for 27 years. I have never bounced a check or been late on a payment. My credit was perfect to say the least. And my reward was that due to my excellent credit, these criminals were able to walk into any establishment and buy what ever they desired on the spot, merely because they had access to my Social Security card. And now if I were to attempt it, I would be treated like a criminal. What kind of system is that? Of course, the lessons I learned were to never have anything on your person with your Social Security number on it. To never write your Social Security number when asked for it. However, sometimes it is completely unavoidable. For instance, I went to school last semester at F.I.U. Your student I.D. number is your Social Security number. You have no choice. Our bank statements has our SS # on it. All you can do is hold your breath and hope that the "bad guys" pass you by this time.

I was relieved when I was informed that the criminal ring had been busted and sent to jail. But my worries began again when I was asked by the D.A. to testify. I told him that I wanted them off the street but that I feared them, as they were a big family that lived in close proximity to my home. They shopped at the same KMart! He tried to reassure me they would not come after me and I tried to believe him. Fortunately, they never called me as a witness, because I found out from Agent Ivey that they actually shot an informant.

In conclusion, it seems to me that with the onset of advanced technology, that we can come up with a system that deters the criminal and protects the victim. I believe the first thing that must be done is to do away with the attachment of Social Security to the identity of someone and their financial welfare. What about thumbprint identification? I know the technology is there. Do you think someone who knowingly is writing with stolen checks would give their thumb print? I may not have the answers and my idea is a shot in the dark, but I do know from my nightmare that the current system is merely an invitation and a ticket for the criminally minded. I implore you to research the alternatives and find a way to protect the honest, hard working citizens of Florida.

Please feel free to contact me to talk about this matter by phone, mail or email. I am eager to help solve this problem in any way that I can.

Thank you for you time and consideration in this matter.

Yours Truly,

MS. VALA B. KODISH